PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-346659
(43)Date of publication of application : 15.12.2005

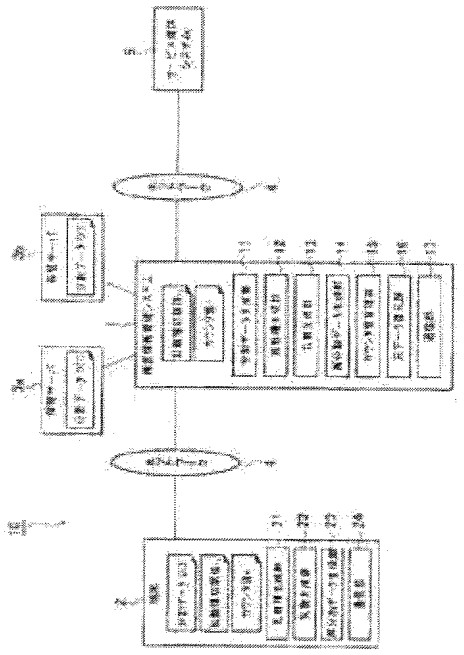
(51)Int.Cl. G06F 12/14
G09C 1/00

(21)Application number : 2004-169004
(22)Date of filing : 07.06.2004

(71)Applicant : NTT COMMUNICATIONS KK
(72)Inventor : OGIWARA TOSHIHIKO
KAGAYA MAKOTO
NOMURA SUSUMU

(54) SECRET INFORMATION MANAGEMENT SYSTEM, SECRET INFORMATION MANAGEMENT METHOD, SECRET INFORMATION MANAGEMENT PROGRAM AND TERMINAL PROGRAM FOR SECRET INFORMATION MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To certainly prevent spoofing even if secret information about a user is leaked to a third party when using service.
SOLUTION: First, in this secret information management system 1, the secret information S is divided into a plurality of pieces of data by use of a secret dispersion method (hereinafter called a secret dispersion method A) by original secret dispersion algorithm, and the division data D are stored in storage servers 3a, 3b and a terminal 2. When using the service, redivision data D' wherein the division data D are synchronized and updated are generated and stored in the secret information management system 1 and the terminal 2. When transmitting the division data D' generated by the terminal 2 to the secret information management system 1 from the terminal 2, the secret information management system 1 restores the original secret information S from each piece of the redivision data D' by use of the secret dispersion method A and transmits the secret information S to a service provision system 5.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-346659
(P2005-346659A)
(43)公開日　平成17年12月15日(2005.12.15)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	510F	5B017
G09C 1/00	G06F 12/14	530P	5J104
	G06F 12/14	540P	
	G09C 1/00	650Z	

審査請求 未請求　請求項の数 16　OL　（全 40 頁）

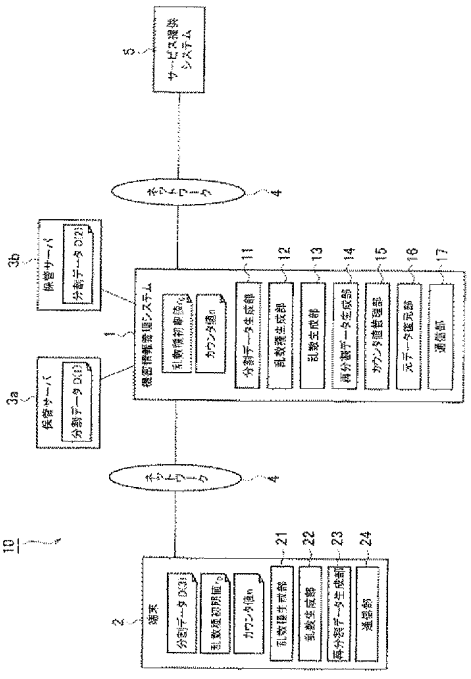
(21)出願番号　特願2004-169004 (P2004-169004)
(22)出願日　平成16年6月7日 (2004.6.7)

(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100098327
弁理士　高松　俊雄

最終頁に続く

(54)【発明の名称】機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラム

(57)【要約】
【課題】サービス利用時に仮にユーザの機密情報が第３者に漏洩したとしても、なりすましを確実に防止することができる。
【解決手段】まず、機密情報管理システム１において独自の秘密分散アルゴリズムによる秘密分散法（以下、秘密分散法Ａとよぶ）を用いて該機密情報Ｓを複数のデータに分割し、該分割データＤをそれぞれ保管サーバ３ａ，３ｂ、端末２に保管させる。サービス利用時は、機密情報管理システム１及び端末２において、分割データＤをそれぞれ同期をとって更新した再分割データＤ’を生成し、保管するとともに、端末２から機密情報管理システム１に対して、端末２で生成した分割データＤ’を送信すると、機密情報管理システム１は、各再分割データＤ’から秘密分散法Ａを用いてもとの機密情報Ｓを復元し、該機密情報Ｓをサービス提供システム５に送信する。
【選択図】図１



【特許請求の範囲】
【請求項1】
利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムであって、
前記秘密分散法は、
前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、
新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、
前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、
所定の初期情報を生成する初期情報生成手段と、
前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶手段と、
前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶手段と、
前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、
新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、
前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶手段と、
前記第１の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第１の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段と、
前記同期情報を更新して前記第２の記憶部に記憶させる同期情報更新手段と、
を有することを特徴とする機密情報管理システム。
【請求項2】
前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、
前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする請求項１記載の機密情報管理システム。
【請求項3】
前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする請求項１又は２記載の機密情報管理システム。
【請求項4】
前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数

部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項１乃至３のいずれか１項に記載の機密情報管理システム。

【請求項5】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項１乃至３のいずれか１項に記載の機密情報管理システム。

【請求項6】

利用者の機密情報を秘密分散法を用いて管理する機密情報管理方法であって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、

所定の初期情報を生成する初期情報生成ステップと、

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶ステップと、

前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶ステップと、

前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、

新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、

前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶ステップと、

前記第１の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第１の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、

前記同期情報を更新して前記第２の記憶部に記憶させる同期情報更新ステップと、

を有することを特徴とする機密情報管理方法。

【請求項7】

利用者の機密情報を秘密分散法を用いて管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割す

るデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、

所定の初期情報を生成する初期情報生成ステップと、

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶ステップと、

前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶ステップと、

前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、

新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、

前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶ステップと、

前記第１の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第１の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、

前記同期情報を更新して前記第２の記憶部に記憶させる同期情報更新ステップと、

を前記コンピュータに実行させることを特徴とする機密情報管理プログラム。

【請求項8】

前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、

前記乱数生成ステップは、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする請求項７記載の機密情報管理プログラム。

【請求項9】

前記データ分割ステップの秘密分散法で用いられた乱数は、真性乱数であることを特徴とする請求項７又は８記載の機密情報管理プログラム。

【請求項10】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項７乃至９のいずれか１項に記載の機密情報管理プログラム。

【請求項11】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式によ

り、各再分割部分データを生成することを特徴とする請求項７乃至９のいずれか１項に記載の機密情報管理プログラム。

【請求項12】

利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムを利用するための端末が読み取り可能な機密情報管理システム用端末プログラムであって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報管理システムは、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、

所定の初期情報を生成する初期情報生成手段と、

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶手段と、

前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶手段と、

前記利用者が前記機密情報を使用する場合には、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、

新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、

前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶手段と、を有し、

前記第１の記憶部に記憶された分割データ及び初期情報を第３の記憶部に記憶するステップと、

前記利用者が前記機密情報を使用するときは、前記機密情報管理システムから前記同期情報を受信するステップと、

前記初期情報及び前記同期情報に基づいて、前記機密情報管理システムで生成された新たな乱数と同じ乱数を生成する乱数生成ステップと、

新たに生成された乱数及び前記秘密分散法を用いて、前記第３の記憶部に記憶された分割データから、再分割データを生成するデータ再分割ステップと、

前記再分割データを前記機密情報管理システムに送信するステップと、

を前記端末に実行させ、前記機密情報管理システムは、送信された再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元し、前記同期情報を更新して前記第２の記憶部に記憶させることを特徴とする機密情報管理システム用端末プログラム。

【請求項13】

前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、

前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、

前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする請求項１２記載の機密情報管理システム用端末プログラム。

【請求項14】

前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする請求項１２又は１３記載の機密情報管理システム用端末プログラム。

【請求項15】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項１２乃至１４のいずれか１項に記載の機密情報管理システム用端末プログラム。

【請求項16】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項１２乃至１４のいずれか１項に記載の機密情報管理システム用端末プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、利用者の機密情報を管理する機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムに関する。

【背景技術】

【0002】

ＩＴ（Information Technology）技術の発展に伴って、パスワード、クレジット番号などが入った携帯電話および携帯情報端末、並びにＰＫＩ秘密鍵が入ったＩＣカードなどを用いて、所望のサービスの提供を受ける機会が増えている。例えば、ユーザのパスワードを使用してログインし、情報を閲覧したり、ユーザのクレジットカード番号を使用して物品購入したりするようなサービスが普及している。

【0003】

尚、この出願に関連する先行技術文献情報としては、次のものがある。

【非特許文献1】電子認証システム推進検討会、“企業間電子商取引システムにおける電子認証システムの仕様に関するガイドライン”、[Online]、［平成１６年５月２０日検索］、インターネット＜ＵＲＬ： http://www.ecom.or.jp/home/gl2.pdf＞

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、ユーザが上述したサービスを利用するときは、インターネット網などオープンなネットワークを介して機密情報（例えば、パスワード、クレジット番号およびＰＫＩ秘密鍵など）を送信することが多いので、第３者に機密情報が漏洩される可能性があるという課題がある。

【0005】

本発明は、上記の課題を解決するためになされたものであり、サービス利用時に仮にユーザの機密情報が第３者に漏洩したとしても、なりすましを確実に防止することができる機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムを提供することを目的とする。

【課題を解決するための手段】

【0006】

上記目的を達成するため、請求項１記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムであって、前記秘密分散法は、前記機密情報を所望

の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、所定の初期情報を生成する初期情報生成手段と、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶手段と、前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶手段と、前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶手段と、前記第１の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第１の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段と、前記同期情報を更新して前記第２の記憶部に記憶させる同期情報更新手段と、を有することを特徴とする。

【0007】

請求項２記載の本発明は、請求項１記載の発明において、前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする。

【0008】

請求項３記載の本発明は、請求項１又は２記載の発明において、前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする。

【0009】

請求項４記載の本発明は、請求項１乃至３のいずれか１項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0010】

請求項５記載の本発明は、請求項１乃至３のいずれか１項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0011】

請求項６記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管

理方法であって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、所定の初期情報を生成する初期情報生成ステップと、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶ステップと、前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶ステップと、前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶ステップと、前記第１の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第１の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、前記同期情報を更新して前記第２の記憶部に記憶させる同期情報更新ステップと、を有することを特徴とする。

【0012】

請求項７記載の本発明は、利用者の機密情報を秘密分散法を用いて管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、所定の初期情報を生成する初期情報生成ステップと、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶ステップと、前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶ステップと、前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、新たに生成された乱数及び前記秘密分散法を用いて、

前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶ステップと、前記第１の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第１の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、前記同期情報を更新して前記第２の記憶部に記憶させる同期情報更新ステップと、を前記コンピュータに実行させることを特徴とする。

【0013】

請求項８記載の本発明は、請求項７記載の発明において、前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、前記乱数生成ステップは、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする。

【0014】

請求項９記載の本発明は、請求項７又は８記載の発明において、前記データ分割ステップの秘密分散法で用いられた乱数は、真性乱数であることを特徴とする。

【0015】

請求項１０記載の本発明は、請求項７乃至９のいずれか１項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0016】

請求項１１記載の本発明は、請求項７乃至９のいずれか１項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0017】

請求項１２記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムを利用するための端末が読み取り可能な機密情報管理システム用端末プログラムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報管理システムは、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、所定の初期情報を生成する初期情報生成手段と、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第１の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第２の記憶部に記憶させるデータ記憶手段と、前記第１の記憶部及び前記第２の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第２の記憶部に記憶させる同期情報記憶手段と、前記利用者が前記機密情報を使用する場合には、前記同期情報及び前記初期情報に基づいて新たに乱数を生

成する乱数生成手段と、新たに生成された乱数及び前記秘密分散法を用いて、前記第２の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、前記第２の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第２の記憶部に記憶させるデータ再記憶手段と、を有し、前記第１の記憶部に記憶された分割データ及び初期情報を第３の記憶部に記憶するステップと、前記利用者が前記機密情報を使用するときは、前記機密情報管理システムから前記同期情報を受信するステップと、前記初期情報及び前記同期情報に基づいて、前記機密情報管理システムで生成された新たな乱数と同じ乱数を生成する乱数生成ステップと、新たに生成された乱数及び前記秘密分散法を用いて、前記第３の記憶部に記憶された分割データから、再分割データを生成するデータ再分割ステップと、前記再分割データを前記機密情報管理システムに送信するステップと、を前記端末に実行させ、前記機密情報管理システムは、送信された再分割データ、及び前記第２の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元し、前記同期情報を更新して前記第１の記憶部に記憶させることを特徴とする。

【0018】

請求項１３記載の本発明は、請求項１２記載の発明において、前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする。

【0019】

請求項１４記載の本発明は、請求項１２又は１３記載の発明において、前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする。

【0020】

請求項１５記載の本発明は、請求項１２乃至１４のいずれか１項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0021】

請求項１６記載の本発明は、請求項１２乃至１４のいずれか１項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【発明の効果】

【0022】

本発明によれば、機密情報を秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるとともに、機密情報を使用するたびに、各分割データを同期をとって更新して再分割データを生成するので、仮にユーザが保持する機密情報の一部が第３者に漏洩したとしても、第３者のなりすましを確実に防止することができ、セキュリティが十分に確保された機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムを提供することができる。

【0023】

特に、本発明における秘密分散法は、機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の

乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するので、機密情報を復元することなく、機密情報を再分割することができるので、ユーザの機密情報をよりセキュアに管理することができる。

【発明を実施するための最良の形態】

【0024】

以下、本発明の実施の形態を図面を用いて説明する。

【0025】

＜システム構成＞

図１は、本発明の実施の形態に係る機密情報管理システム１が適用されるコンピュータシステム１０全体の概略構成を示すブロック図である。

【0026】

図１に示す機密情報管理システム１は、通信ネットワーク４を介してユーザが備えるクライアント端末２（以下、単に端末とよぶ）と接続されているとともに、通信ネットワーク４を介してユーザに所定のサービスを提供するサービス提供システム５と接続されている。また、機密情報管理システム１は、ハードウェア的に互いに独立した複数（本実施の形態では２とする）のデータ保管用サーバコンピュータ（以下、単に保管サーバとよぶ）３ａ，３ｂと接続されている。

【0027】

尚、本実施の形態における機密情報とは、ユーザがサービス提供システム５を利用するために必要なパスワード、クレジットカード番号、ＰＫＩ秘密鍵などの個人情報をいう。

【0028】

上記構成のコンピュータシステム１０においては、端末２がサービス提供システム５から所定のサービスを受けるには、まず、機密情報Ｓを機密情報管理システム１に送信（通信内容の漏洩を防止するため、オープンなネットワークではなく、セキュアな通信ネットワーク４ａ、例えば、ＬＡＮ、ＩＰ－ＶＰＮ、専用線、電話回線などによる）又は送付（例えば、郵便などの手段による）し、機密情報管理システム１において後述する独自の秘密分散アルゴリズムによる秘密分散法（以下、秘密分散法Ａとよぶ）を用いて該機密情報Ｓを複数のデータに分割し、該分割データを保管サーバ３ａ，３ｂおよび端末２にそれぞれに送信（セキュアな通信ネットワーク４ａによる）又は送付し、保管させるようになっている。この結果、機密情報Ｓが機密情報管理システム１に登録されたことになり、ユーザはサービス利用の準備が整ったことになる。尚、図１では、機密情報管理システム１は、端末２からの機密情報Ｓを３つの分割データD(1)，D(2)，D(3)に分割し、それぞれを複数の保管サーバ３ａ，３ｂおよび端末２に保管するようになっている。

【0029】

また、サービス利用時は、機密情報管理システム１及び端末２において、分割データD(1)，D(2)，D(3)をそれぞれ同期をとって更新した再分割データD’(1)，D’(2)，D’(3)を生成し、保管するので、端末２から機密情報管理システム１に対して、分割データD’(3)を送信（オープンな通信ネットワーク４ｂ、例えば、インターネット網などによる）すると、機密情報管理システム１は、送信された分割データD’(3)および保管サーバ３ａ，３ｂの再分割データD’(1),D’(2)のうち任意の２つから秘密分散法Ａを用いてもとの機密情報Ｓを復元し、該機密情報Ｓをサービス提供システム５に送信するようになっている。これにより、ユーザは、サービス提供システム５から所定のサービスの提供を受けることができる。

【0030】

尚、本実施の形態においては、機密情報Ｓを３分割して保管する場合を例に説明するが、本発明は機密情報Ｓを３分割する場合に限定されるわけではなく、ｎ分割（ｎ＝２以上の整数）の場合にも適用されるものである。また、端末２に送信される分割データは１つとは限らず複数であってもよいものである。さらに、本実施の形態においては、分割データD(1),D(2)を保管サーバ３、分割データD(3)を利用端末２に割り当てたが、どの分割デ

ータをどの保管サーバ３および利用端末２に割り当ててもよいものである。

【0031】

機密情報管理システム１は、詳しくは、機密情報Ｓから秘密分散法Ａを用いて複数の分割データD(1)，D(2),D(3)に分割する分割データ生成部１１、再分割データD’(1)，D’(2)を生成するために使用される乱数Ｒ’のシード（乱数生成の種となる情報）r_nを乱数種初期値r_0及びカウンタ値ｎを用いて生成する乱数種生成部１２、機密情報Ｓから分割データD(1)，D(2)，D(3)を生成するために使用される真性乱数Ｒを生成するとともに、再分割データD’(1)，D’(2)を生成するために使用される乱数Ｒ’を上述したシードr_n及び所定の疑似乱数アルゴリズムＧに基づいて生成する乱数生成部１３、ユーザがサービス提供システム５から所定のサービスを受ける際に、秘密分散法Ａを用いて分割データD(1)，D(2)から再分割データD’(1)，D’(2)を生成する再分割データ生成部１４、端末２と同期をとって再分割データD’(1)，D’(2)を生成するために必要なカウンタ値ｎを初期設定するとともに、機密情報Ｓをサービス提供システム５で使用するたびにカウンタ値ｎを減算して更新するカウンタ値管理部１５、複数の再分割データD’(1)，D’(2)，D’(3)のいずれか２つから秘密分散法Ａを用いて元データ（機密情報）Ｓを復元する元データ復元部１６、並びに端末２、保管サーバ３ａ，３ｂ、及びサービス提供システム５それぞれとデータの送受信を行う通信部１７を具備する構成となっている。

【0032】

端末２は、詳しくは、ユーザがサービス提供システム５から所定のサービスを受ける際に、機密情報管理システム１から送信されたカウンタ値ｎ及び乱数種初期値r_0を用いて、再分割データD’(3)を生成するために使用される乱数Ｒ’のシード（乱数生成の種となる情報）r_nを生成する乱数種生成部２２、再分割データD’(3)を生成するために使用される乱数Ｒ’を上述したシードr_n及び所定の疑似乱数アルゴリズムＧに基づいて生成する乱数生成部２２、上述した乱数Ｒ’及び機密情報管理システム１から送信された分割データD(3)から、秘密分散法Ａを用いて再分割データD’(3)を生成する再分割データ生成部２３、並びに、機密情報管理システム１及びサービス提供システム５それぞれとデータの送受信を行う通信部２４を具備する構成となっている。

【0033】

尚、端末２は、ユーザが携行可能な携帯情報端末、携帯電話、ＩＣカードなどの携帯記憶媒体などが想定されるが、他にモバイルを用途としないコンピュータ機器であってもよいものである。

【0034】

ここで、上述した機密情報管理システム１、端末２、保管サーバ３ａ，３ｂおよびサービス提供システム５は、それぞれ少なくとも演算機能および制御機能を備えた中央演算装置（ＣＰＵ）、プログラムやデータを格納する機能を有するＲＡＭ等からなる主記憶装置（メモリ）を有する電子的な装置から構成されているものである。また、上記装置およびシステムは、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。尚、本実施の形態においては、保管サーバ３ａ，３ｂ及びサービス提供システム５をそれぞれ、機密情報管理システム１と物理的に独立したサーバ装置とし、各装置がネットワーク接続された形態としているが、物理的に機密情報管理システム１と一体化されたサーバ装置としてもよいものである。

【0035】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0036】

＜秘密分散法Ａ＞

ここで、本実施の形態における独自の秘密分散アルゴリズムによる秘密分散法Ａについ

て説明する。

【0037】

本実施形態における元データ（機密情報Ｓに相当する）の分割および復元では、元データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するが、この場合の処理単位ビット長は任意の値に設定することができ、元データを処理単位ビット長毎に区分けして、この元部分データから分割部分データを分割数より１少ない数ずつ生成するので、元データのビット長が処理単位ビット長の（分割数-1）倍の整数倍に一致しない場合は、元データの末尾の部分に０を埋めるなどして元データのビット長を処理単位ビット長の（分割数-1）倍の整数倍に合わせることにより本実施形態を適用することができる。

【0038】

また、上述した乱数も（分割数-1）個の元部分データの各々に対応して処理単位ビット長のビット長を有する（分割数-1）個の乱数部分データとして乱数生成部１３から生成される。すなわち、乱数は処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する（分割数-1）個の乱数部分データとして生成される。更に、元データは処理単位ビット長に基づいて所望の分割数の分割データに分割されるが、この分割データの各々も（分割数-1）個の元部分データの各々に対応して処理単位ビット長のビット長を有する（分割数-1）個の分割部分データとして生成される。すなわち、分割データの各々は、処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する（分割数-1）個の分割部分データとして生成される。

【0039】

なお、以下の説明では、上述した元データ、乱数、分割データ、分割数および処理単位ビット長をそれぞれS,R,D,nおよびbで表すとともに、また複数のデータや乱数などのうちの１つを表わす変数としてi(=1～n)およびj(=1～n-1)を用い、（分割数n-1）個の元部分データ、（分割数n-1）個の乱数部分データ、および分割数n個の分割データDのそれぞれのうちの１つをそれぞれS（j),R(j)およびD(i)で表記し、更に各分割データD(i)を構成する複数(n-1)の分割部分データをD(i,j)で表記するものとする。すなわち、S（j)は、元データSの先頭から処理単位ビット長毎に区分けして１番から順に採番した時のj番目の元部分データを表すものである。

【0040】

この表記を用いると、元データ、乱数データ、分割データとこれらをそれぞれ構成する元部分データ、乱数部分データ、分割部分データは、次のように表記される。

【0041】

元データS=(n-1)個の元部分データS(j)

=S(1),S(2),…,S(n-1)

乱数R=(n-1)個の乱数部分データR(j)

=R(1),R(2),…,R(n-1)

n個の分割データD(i)=D(1),D(2),…,D(n)

各分割部分データD(i,j)

$$=\begin{matrix} D(1,1),D(1,2),\cdots,D(1,n-1) \\ D(2,1),D(2,2),\cdots,D(2,n-1) \\ \cdots \quad \cdots \quad \cdots \\ D(n,1),D(n,2),\cdots,D(n,n-1) \end{matrix}$$

(i=1～n)，(j=1～n-1)

本実施形態は、上述したように処理単位ビット長毎に区分けされる複数の部分データに対して元部分データと乱数部分データの排他的論理和演算（XOR）を行って、詳しくは、元部分データと乱数部分データの排他的論理和演算（XOR）からなる定義式を用いて、元データの分割を行うことを特徴とするものであり、上述したデータ分割処理に多項式や剰余演算を用いる方法に比較して、コンピュータ処理に適したビット演算である排他的論理和（XOR）演算を用いることにより高速かつ高性能な演算処理能力を必要とせず、大容量

のデータに対しても簡単な演算処理を繰り返して分割データを生成することができるとともに、また分割データの保管に必要となる記憶容量も分割数に比例した倍数の容量よりも小さくすることができる。更に、任意に定めた一定の長さ毎にデータの先頭から順に演算処理を行うストリーム処理により分割データが生成される。

【0042】

なお、本実施形態で使用する排他的論理和演算（XOR）は、以下の説明では、「＊」なる演算記号で表すことにするが、この排他的論理和演算のビット毎の演算規則での各演算結果は下記のとおりである。

【0043】

0 ＊ 0 の演算結果は 0
0 ＊ 1 の演算結果は 1
1 ＊ 0 の演算結果は 1
1 ＊ 1 の演算結果は 0

また、XOR演算は交換法則、結合法則が成り立つ。すなわち、

a*b=b*a
(a*b)*c=a*(b*c)が成り立つことが数学的に証明される。

【0044】

また、a*a=0,a*0=0*a=aが成り立つ。

【0045】

ここでa,b,cは同じ長さのビット列を表し、0はこれらと同じ長さですべて「0」からなるビット列を表す。

【0046】

次に、フローチャートなどの図面も参照して、本実施の形態における秘密分散法Ａの作用について説明するが、この説明の前に図２乃至６、図８および図１０に示す記号の定義について説明する。

【0047】

（１）$\Pi_{i=1}^{n}A(i)$は、A(1)*A(2)*…A(n)を意味するものとする。

【0048】

（２）c(j,i,k)を(n-1)×(n-1)行列であるU[n-1,n-1]×(P[n-1,n-1])^(j-1)のi行k列の値と定義する。

【0049】

このときQ(j,i,k)を下記のように定義する。

【0050】

c(j,i,k)=1 のとき Q(j,i,k)=R((n-1)×m+k)
c(j,i,k)=0 のとき Q(j,i,k)=0

ただし、mはm≧0の整数を表す。

【0051】

（３）U[n,n]とは、n×n行列であって、i行j列の値をu(i,j)で表すと、

i+j<=n+1 のとき u(i,j)=1
i+j>n+1　のとき u(i,j)=0

である行列を意味するものとし、「上三角行列」ということとする。具体的には下記のような行列である。

【数1】

$$U[3,3]=\begin{pmatrix}1&1&1\\1&1&0\\1&0&0\end{pmatrix}\qquad U[4,4]=\begin{pmatrix}1&1&1&1\\1&1&1&0\\1&1&0&0\\1&0&0&0\end{pmatrix}$$

【0052】

（４）P[n,n]とは、n×n行列であって、i行j列の値をp(i,j)で表すと、

j=i+1　　のとき p(i,j)=1

i=1,j=n　のとき p(i,j)=1

上記以外のとき　p(i,j)=0

である行列を意味するものとし、「回転行列」ということとする。具体的には下記のような行列であり、他の行列の右側からかけると当該他の行列の１列目を２列目へ、２列目を３列目へ、…,n-1列目をn列目へ、n列目を１列目へ移動させる作用がある。つまり、行列Pを他の行列に右側から複数回かけると、その回数分だけ各列を右方向へ回転させるように移動させることができる。

【数2】

$$P[3,3]=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\qquad U[4,4]=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{pmatrix}$$

【0053】

（５）A,Bをn×n行列とすると、A×Bとは行列AとBの積を意味するものとする。行列の成分同士の計算規則は通常の数学で用いるものと同じである。

【0054】

（６）Aをn×n行列とし、iを整数とすると、A^iとは行列Aのi個の積を意味するものとする。また、A^0とは単位行列Eを意味するものとする。

【0055】

（７）単位行列E[n,n]とは、n×n行列であって、i行j列の値をe(i,j)で表すと、

i=j　　のとき e(i,j)=1

上記以外のとき e(i,j)=0

である行列を意味するものとする。具体的には下記のような行列である。Aを任意のn×n行列とすると

A×E=E×A=A

となる性質がある。

【数3】

$$E[3,3]=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\qquad E[4,4]=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

【0056】
次に、図２に示すフローチャートおよび図３および図４に示す具体的データなどを参照して、まず元データSの分割処理について説明する。これは、機密情報管理システム１の分割データ生成部１１の機能を説明するものである。
【0057】
まず、元データSを機密情報管理システム１に与える（図２のステップＳ２０１）。なお、本例では、元データSは、１６ビットの「10110010 00110111」とする。
【0058】
次に、機密情報管理システム１は、分割数nとして３と指示する（ステップＳ２０３）。なお、この分割数n=3に従って機密情報管理システム１で生成される３個の分割データをD(1),D(2),D(3)とする。この分割データD(1),D(2),D(3)は、すべて元データのビット長と同じ１６ビット長のデータである。
【0059】
それから、元データSを分割するために使用される処理単位ビット長bを８ビットと決定する（ステップＳ２０５）。この処理単位ビット長bは、利用者が端末２から機密情報管理システム１に対して指定してもよいし、または機密情報管理システム１において予め定められた値を用いてもよい。なお、処理単位ビット長bは、任意のビット数でよいが、ここでは元データSを割り切れることができる８ビットとしている。従って、上記１６ビットの「10110010 00110111」の元データSは、８ビットの処理単位ビット長で区分けされた場合の２個の元分割データS(1)およびS(2)は、それぞれ「10110010」および「00110111」となる。
【0060】
次のステップＳ２０７では、元データSのビット長が8×2の整数倍であるか否かを判定し、整数倍でない場合には、元データSの末尾を０で埋めて、8×2の整数倍に合わせる。なお、本例のように処理単位ビット長bが８ビットおよび分割数nが３に設定された場合における分割処理は、元データSのビット長として１６ビットに限られるものでなく、処理単位ビット長b×(分割数n-1)=8×2の整数倍の元データSに対して有効なものである。
【0061】
次に、ステップＳ２０９では、変数m、すなわち上述した整数倍を意味する変数mを０に設定する。本例のように、元データSが処理単位ビット長b×(分割数n-1)=8×2=16ビットである場合には、変数mは０であるが、２倍の３２ビットの場合には、変数mは１となり、３倍の４８ビットの場合には、変数mは２となる。
【0062】
次に、元データSの8×2×m+1ビット目から8×2ビット分のデータが存在するか否かが判定される（ステップＳ２１１）。これは、このステップＳ２１１以降に示す分割処理を元データSの変数mで特定される処理単位ビット長b×(分割数n-1)=8×2=16ビットに対して行った後、元データSとして次の１６ビットがあるか否かを判定しているものである。本例のように元データSが１６ビットである場合には、１６ビットの元データSに対してステップＳ２１１以降の分割処理を１回行うと、後述するステップＳ２１９で変数mが+1されるが、本例の元データSでは変数mがm+1の場合に相当する１７ビット以降のデータは存在しないので、ステップＳ２１１からステップＳ２２１に進むことになるが、今の場合は、変

数mは０であるので、元データSの8×2×m+1ビット目は、8×2×0+1=1となり、元データSの１６ビットの１ビット目から8×2ビット分にデータが存在するため、ステップＳ２１３に進む。

【0063】

ステップＳ２１３では、変数jを１から２(=分割数n-1)まで変えて、元データSの8×(2×m+j-1)+1ビット目から８ビット分(=処理単位ビット長)のデータを元部分データS(2×m+j)に設定し、これにより元データSを処理単位ビット長で区分けした２(分割数n-1)個の元部分データS(1),S(2)を次のように生成する。

【0064】

元データS=S(1),S(2)

第１の元部分データS(1)=「10110010」

第２の元部分データS(2)=「00110111」

次に、変数jを１から２(=分割数n-1)まで変えて、乱数部分データR(2×m+j)に乱数生成部１３から発生する８ビットの長さの乱数を設定し、これにより乱数Rを処理単位ビット長で区分けした２(分割数n-1)個の乱数部分データR(1),R(2)を次のように生成する（ステップＳ２１５）。

【0065】

乱数R=R(1),R(2)

第１の乱数部分データR(1)=「10110001」

第２の乱数部分データR(2)=「00110101」

次に、ステップＳ２１７において、変数iを１から３(=分割数n)まで変えるとともに、更に各変数iにおいて変数jを１から２(=分割数n-1)まで変えながら、ステップＳ２１７に示す分割データを生成するための元部分データと乱数部分データの排他的論理和からなる定義式により複数の分割データD(i)の各々を構成する各分割部分データD(i,2×m+j)を生成する。この結果、次に示すような分割データDが生成される。

【0066】

分割データD

=３個の分割データD(i)=D(1),D(2),D(3)

第１の分割データD(1)

=２個の分割部分データD(1,j)=D(1,1),D(1,2)

=「00110110」,「10110011」

第２の分割データD(2)

=２個の分割部分データD(2,j)=D(2,1),D(2,2)

=「00000011」,「00000010」

第３の分割データD(3)

=２個の分割部分データD(3,j)=D(3,1),D(3,2)

=「10110001」,「00110101」

なお、各分割部分データ(i,j)を生成するためのステップＳ２１７に示す定義式は、本例のように分割数n=3の場合には、具体的には図４に示す表に記載されているものとなる。図４に示す表から、分割部分データD(1,1)を生成するための定義式はS(1)*R(1)*R(2)であり、D(1,2)の定義式はS(2)*R(1)*R(2)であり、D(2,1)の定義式はS(1)*R(1)であり、D(2,2)の定義式はS(2)*R(2)であり、D(3,1)の定義式はR(1)であり、D(3,2)の定義式はR(2)である。また、図４に示す表にはm>0の場合の任意の整数についての一般的な定義式も記載されている。

【0067】

このように整数倍を意味する変数m=0の場合について分割データDを生成した後、次に変数mを１増やし（ステップＳ２１９）、ステップＳ２１１に戻り、変数m+1に該当する元データSの１７ビット以降について同様の分割処理を行おうとするが、本例の元データSは１６ビットであり、１７ビット以降のデータは存在しないので、ステップＳ２１１からステップＳ２２１に進み、上述したように生成した分割データD(1),D(2),D(3)を保管サーバ３

及び端末２にそれぞれ保存して、分割処理を終了する。なお、このように保管された分割データD(1),D(2),D(3)はそれぞれ単独では元データが推測できない。

【0068】

ここで、上述した図２のフローチャートのステップＳ２１７における定義式による分割データの生成処理、具体的には分割数n=3の場合の分割データの生成処理について詳しく説明する。

【0069】

まず、整数倍を意味する変数m=0の場合には、ステップＳ２１７に示す定義式から各分割データD(i)=D(1)～D(3)の各々を構成する各分割部分データD(i,2×m+j)=D(i,j)(i=1～3,j=1～2)は、次のようになる。

【0070】

D(1,1)=S(1)*Q(1,1,1)*Q(1,1,2)
D(1,2)=S(2)*Q(2,1,1)*Q(2,1,2)
D(2,1)=S(1)*Q(1,2,1)*Q(1,2,2)
D(2,2)=S(2)*Q(2,2,1)*Q(2,2,2)
D(3,1)=R(1)
D(3,2)=R(2)

上記の６つの式のうち上から４つの式に含まれるQ(j,i,k)を具体的に求める。

【0071】

これはc(j,i,k)を2×2行列であるU[2,2]×(P[2,2])^(j-1)のi行k列の値としたとき下記のように定義される。

【0072】

c(j,i,k)=1 のとき Q(j,i,k)=R(k)
c(j,i,k)=0 のとき Q(j,i,k)=0

ここで、

j=1のときは

【数4】

$$U[2,2]\times(P[2,2])^{(j-1)} = U[2,2]\times(P[2,2])^{0}$$

$$= U[2,2]\times E[2,2]$$

$$= U[2,2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

【0073】

j=2のときは

【数5】

$$U[2,2]\times(P[2,2])^{(j-1)} = U[2,2]\times(P[2,2])^{1}$$

$$= U[2,2]\times P[2,2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

【0074】
これを用いると、各分割部分データD(i,j)は次のような定義式により生成される。
【0075】
D(1,1)=S(1)*Q(1,1,1)*Q(1,1,2)=S(1)*R(1)*R(2)
D(1,2)=S(2)*Q(2,1,1)*Q(2,1,2)=S(2)*R(1)*R(2)
D(2,1)=S(1)*Q(1,2,1)*Q(1,2,2)=S(1)*R(1)*0=S(1)*R(1)
D(2,2)=S(2)*Q(2,2,1)*Q(2,2,2)=S(2)*0*R(2)=S(2)*R(2)
上述した各分割部分データD(i,j)を生成するための定義式は、図３にも図示されている。
【0076】
図３は、上述したように１６ビットの元データSを８ビットの処理単位ビット長に基づいて分割数n=3で３分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。
【0077】
ここで、上述した定義式により分割データD(1),D(2),D(3)および各分割部分データD(1,1),D(1,2),D(2,1),D(2,2),D(3,1),D(3,2)を生成する過程と定義式の一般形について説明する。
【0078】
まず、第１の分割データD(1)に対しては、第１の分割部分データD(1,1)は、上述した定義式S(1)*R(1)*R(2)で定義され、第２の分割部分データD(1,2)は定義式S(2)*R(1)*R(2)で定義される。なお、この定義式の一般形は、D(1,j)に対してはS(j)*R(j)*R(j+1)であり、D(1,j+1)に対してS(j+1)*R(j)*R(j+1)である（jは奇数とする）。定義式に従って計算すると、D(1,1)は00110110, D(1,2)は10110011となるので、D(1)は00110110 10110011である。なお、定義式の一般形は、図４にまとめて示されている。
【0079】
また、第２の分割データD(2)に対しては、D(2,1)はS(1)*R(1)で定義され、D(2,2)はS(2)*R(2)で定義される。この定義式の一般形は、D(2,j)に対してはS(j)*R(j)であり、D(2,j+1)に対してはS(j+1)*R(j+1)である（jは奇数とする）。定義式に従って計算すると、D(2,1)は00000011, D(2,2)は00000010となるので、D(2)は00000011 00000010である。
【0080】
更に第３の分割データD(3)に対しては、D(3,1)はR(1)で定義され、D(3,2)はR(2)で定義される。この定義式の一般形は、D(3,j)に対してはR(j)であり、D(3,j+1)に対してはR(j+1)である（jは奇数とする）。定義式に従って計算すると、D(3,1)は10110001, D(3,2)は00110101となるので、D(3)は10110001 00110101である。
【0081】
上記説明は、S,R,D(1),D(2),D(3)の長さを１６ビットとしたが、データの先頭から上記分割処理を繰り返すことにより、どのような長さの元データSからでも分割データD(1),D(

2),D(3)を生成することができる。また、処理単位ビット長bは任意にとることができ、元データSの先頭から順にb×2の長さ毎に上記分割処理を繰り返すことにより任意の長さの元データ、具体的には処理単位ビット長b×2の整数倍の長さの元データに対して適用することができる。なお、元データSの長さが処理単位ビット長b×2の整数倍でない場合は、例えば、データ末尾の部分を０で埋めるなどして元データSの長さを処理単位ビット長b×2の整数倍に合わせることにより上述した本実施形態の分割処理を適用することができる。

【0082】

次に、図３の右側に示す表を参照して、分割データから元データを復元する処理について説明する。尚、機密情報管理システム１の元データ復元部１６は、この処理を行うのではなく、後述する再分割データから元データを復元するものであるが、以下、分割データD(1),D(2),D(3)から元データSを復元できることを示す。

【0083】

まず、分割部分データD(2,1),D(3,1)から第１の元部分データS(1)を次のように生成することができる。

【0084】

D(2,1)*D(3,1)=(S(1)*R(1))*R(1)
=S(1)*(R(1)*R(1))
=S(1)*0
=S(1)

具体的に計算すると、D(2,1)は00000011，D(3,1)は10110001なので、S(1)は10110010となる。

【0085】

また、別の分割部分データから次のように第２の元部分データS(2)を生成することができる。

【0086】

D(2,2)*D(3,2)=(S(2)*R(2))*R(2)
=S(2)*(R(2)*R(2))
=S(2)*0
=S(2)

具体的に計算すると、D(2,2)は00000010，D(3,2)は00110101なので、S(2)は00110111となる。

【0087】

一般に、jを奇数として、

D(2,j)*D(3,j)=(S(j)*R(j))*R(j)
=S(j)*(R(j)*R(j))
=S(j)*0
=S(j)

であるから、D(2,j)*D(3,j)を計算すれば、S(j)が求まる。

【0088】

また、一般に、jを奇数として、

D(2,j+1)*D(3,j+1)=(S(j+1)*R(j+1))*R(j+1)
=S(j+1)*(R(j+1)*R(j+1))
=S(j+1)*0
=S(j+1)

であるから、D(2,j+1)*D(3,j+1)を計算すれば、S(j+1)が求まる。

【0089】

次に、D(1),D(3)を取得してSを復元する場合には、次のようになる。

【0090】

D(1,1)*D(3,1)*D(3,2)=(S(1)*R(1)*R(2))*R(1)*R(2) =S(1)*(R(1)*R(1))*(R(2)*R(2))

=S(1)*0*0
=S(1)

であるから、D(1,1)*D(3,1)*D(3,2)を計算すれば、S(1)が求まる。具体的に計算すると、D(1,1)は00110110，D(3,1)は10110001，D(3,2)は00110101なので、S(1)は10110010となる。

【0091】

また同様に、

D(1,2)*D(3,1)*D(3,2)=(S(2)*R(1)*R(2))*R(1)*R(2)
=S(2)*(R(1)*R(1))*(R(2)*R(2))
=S(2)*0*0
=S(2)

であるから、D(1,2)*D(3,1)*D(3,2)を計算すれば、S(2)が求まる。具体的に計算すると、D(1,2)は10110011，D(3,1)は10110001，D(3,2)は00110101なので、S(2)は00110111となる。

【0092】

一般に、jを奇数として、

D(1,j)*D(3,j)*D(3,j+1)=(S(j)*R(j)*R(j+1))*R(j)*R(j+1)
=S(j)*(R(j)*R(j))*(R(j+1)*R(j+1))
=S(j)*0*0
=S(j)

であるから、D(1,j)*D(3,j)*D(3,j+1)を計算すれば、S(j)が求まる。

【0093】

また、一般に、jを奇数として、

D(1,j+1)*D(3,j)*D(3,j+1)=(S(j+1)*R(j)*R(j+1))*R(j)*R(j+1)
=S(j+1)*(R(j)*R(j))*(R(j+1)*R(j+1))
=S(j+1)*0*0
=S(j+1)

であるから、D(1,j+1)*D(3,j)*D(3,j+1)を計算すれば、S(j+1)が求まる。

【0094】

次に、D(1),D(2)を取得してSを復元する場合には、次のようになる。

【0095】

D(1,1)*D(2,1)=(S(1)*R(1)*R(2))*(S(1)*R(1))
=(S(1)*S(1))*(R(1)*R(1))*R(2)
=0*0*R(2)
=R(2)

であるから、D(1,1)*D(2,1)を計算すれば、R(2)が求まる。具体的に計算すると、D(1,1)は00110110，D(2,1)は00000011なので、R(2)は00110101となる。

【0096】

また同様に、

D(1,2)*D(2,2)=(S(2)*R(1)*R(2))*(S(2)*R(2))
=(S(2)*S(2))*R(1)*(R(2)*R(2))
=0*R(1)*0
=R(1)

であるから、D(1,2)*D(2,2)を計算すれば、R(1)が求まる。具体的に計算すると、D(1,2)は10110011，D(2,2)は00000010なので、R(1)は10110001となる。

【0097】

このR(1),R(2)を使用してS(1),S(2)を求める。

【0098】

D(2,1)*R(1)=(S(1)*R(1))*R(1)
=S(1)*(R(1)*R(1))

=S(1)*0
=S(1)

であるから、D(2,1)*R(1)を計算すれば、S(1)が求まる。具体的に計算すると、D(2,1)は00000011，R(1)は10110001なので、S(1)は10110010となる。

【0099】

また同様に、

D(2,2)*R(2)=(S(2)*R(2))*R(2)
=S(2)*(R(2)*R(2))
=S(2)*0
=S(2)

であるからD(2,2)*R(2)を計算すればS(2)が求まる。具体的に計算するとD(2,2)は00000010，R(2)は00110101なので、S(2)は00110111となる。

【0100】

一般に、jを奇数として、

D(1,j)*D(2,j)=(S(j)*R(j)*R(j+1))*(S(j)*R(j))
=(S(j)*S(j))*(R(j)*R(j))*R(j+1)
=0*0*R(j+1)
=R(j+1)

であるからD(1,j)*D(2,j)を計算すればR(j+1)が求まる。

【0101】

また同様に、

D(1,j+1)*D(2,j+1)=(S(j+1)*R(j)*R(j+1))*(S(j+1)*R(j+1))
=(S(j+1)*S(j+1))*R(j)*(R(j+1)*R(j+1))
=0*R(j)*0
=R(j)

であるからD(1,j+1)*D(2,j+1)を計算すればR(j)が求まる。

【0102】

このR(j),R(j+1)を使用してS(j),S(j+1)を求める。

【0103】

D(2,j)*R(j)=(S(j)*R(j))*R(j)
=S(j)*(R(j)*R(j))
=S(j)*0
=S(j)

であるからD(2,j)*R(j)を計算すればS(j)が求まる。

【0104】

また同様に、

D(2,j+1)*R(j+1)=(S(j+1)*R(j+1))*R(j+1)
=S(j+1)*(R(j+1)*R(j+1))
=S(j+1)*0
=S(j+1)

であるからD(2,j+1)*R(j+1)を計算すればS(j+1)が求まる。

【0105】

上述したように、元データの先頭から処理単位ビット長bに基づいて分割処理を繰り返し行って、分割データを生成した場合には、３つの分割データD(1),D(2),D(3)のすべてを用いなくても、３つの分割データのうち、２つの分割データを用いて上述したように元データを復元することができる。

【0106】

尚、本実施の形態に係る機密情報管理システム１においては、３つの分割データD(1),D(2),D(3)を生成するようになっていたので、分割数が３の場合について説明したが、秘密分散法Ａは、分割数がｎの場合にも適用できるものである。

【0107】
次に、図５に示すフローチャートを参照して、分割数がnで、処理単位ビット長がbである場合の一般的な分割処理について説明する。
【0108】
まず、元データSを機密情報管理システム１に与える（ステップＳ４０１）。また、機密情報管理システム１に、分割数n(n≧3である任意の整数)を指示する（ステップＳ４０３）。処理単位ビット長bを決定する（ステップＳ４０５）。なお、bは０より大きい任意の整数である。次に、元データSのビット長がb×(n-1)の整数倍であるか否かを判定し、整数倍でない場合には、元データSの末尾を０で埋める（ステップＳ４０７）。また、整数倍を意味する変数mを０に設定する（ステップＳ４０９）。
【0109】
次に、元データSのb×(n-1)×m+1ビット目からb×(n-1)ビット分のデータが存在するか否かが判定される（ステップＳ４１１）。この判定の結果、データが存在しない場合は、ステップＳ４２１に進むことになるが、今の場合は、ステップＳ４０９で変数mは０に設定された場合であるので、データが存在するため、ステップＳ４１３に進む。
【0110】
ステップＳ４１３では、変数jを１からn-1まで変えて、元データSのb×((n-1)×m+j-1)+1ビット目からbビット分のデータを元部分データS((n-1)×m+j)に設定する処理を繰り返し、これにより元データSを処理単位ビット長bで区分けした(n-1)個の元部分データS(1),S(2),…S(n-1)が生成される。
【0111】
次に、変数jを１からn-1まで変えて、乱数部分データR((n-1)×m+j)に乱数生成部１３から発生する処理単位ビット長bの乱数を設定し、これにより乱数Rを処理単位ビット長bで区分けしたn-1個の乱数部分データR(1),R(2),…R(n-1)が生成される（ステップＳ４１５）。
【0112】
次に、ステップＳ４１７において、変数iを１からnまで変えるとともに、更に各変数iにおいて変数jを１からn-1まで変えながら、ステップＳ４１７に示す分割データを生成するための定義式により複数の分割データD(i)の各々を構成する各分割部分データD(i,(n-1)×m+j)を生成する。この結果、次に示すような分割データDが生成される。
【0113】
分割データD
=n個の分割データD(i)=D(1),D(2),…D(n)
第１の分割データD(1)
=n-1個の分割部分データD(1,j)=D(1,1),D(1,2),…D(1,n-1)
第２の分割データD(2)
=n-1個の分割部分データD(2,j)=D(2,1),D(2,2),…D(2,n-1)
… … …
… … …
第nの分割データD(n)
=n-1個の分割部分データD(n,j)=D(n,1),D(n,2),…D(n,n-1)
このように変数m=0の場合について分割データDを生成した後、次に変数mを１増やし（ステップＳ４１９）、ステップＳ４１１に戻り、変数m=1に該当する元データSのb×(n-1)ビット以降について同様の分割処理を行う。最後にステップＳ４１１の判定の結果、元データSにデータがなくなった場合、ステップＳ４１１からステップＳ４２１に進み、上述したように生成した分割データD(1), …,D(n)を保管サーバ３および端末２にそれぞれ保存して、分割処理を終了する。
【0114】
さて、上述した実施形態においては、個々の分割データのみから、それを構成する部分データ間の演算を行うことによって乱数成分が失われる場合がある。即ち、例えば３分割

の場合、各分割部分データは次のように定義される。

【0115】

D(1,1)=S(1)*R(1)*R(2)，　D(1,2)=S(2)*R(1)*R(2)，…

D(2,1)=S(1)*R(1)，　D(2,2)=S(2)*R(2)，…

D(3,1)=R(1)，D(3,2)=R(2)，…

D(1)について見ると、例えば、D(1,1)、D(1,2)が取得できると、

D(1,1)*D(1,2)=(S(1)*R(1)*R(2))*(S(2)*R(1)*R(2))

=S(1)*S(2)*((R(1)*R(1))*((R(2)*R(2))

=S(1)*S(2)*0*0

=S(1)*S(2)

となる。一般にはD(1,j)*D(1,j+1)=S(j)*S(j+1)である。ここでｊはｊ＝２×ｍ＋１、ｍはｍ≧０の任意の整数である。

【0116】

D(1,1)、D(1,2)は、上記の定義より、元データと乱数の演算により生成されたものであり、D(1,1)、D(1,2)それぞれを見ても元データの内容は分からないが、D(1,1)＊D(1,2)の演算を行うことによりS(1)*S(2)が算出される。これは元データそのものではないが、乱数成分を含んでいない。

【0117】

このように乱数成分が失われると、個々の元部分データについて、例えばS(2)の一部が既知である場合にはS(1)の一部が復元可能となるので、安全ではないと考えられる。例えば、元データが標準化されたデータフォーマットに従ったデータであって、S(2)がそのデータフォーマット中のヘッダ情報やパディング（例えば、データ領域の一部を０で埋めたもの）などを含む部分であった場合には、これらのデータフォーマット固有のキーワードや固定文字列などを含むため、その内容は予測され得る。また、S(2)のうち既知の部分とS(1)*S(2)の値から、S(1)の一部が復元可能である。

【0118】

この問題を解決する方法は以下の通りである。図６におけるD(1,j+1)とD(2,j+1)は、図４におけるD(1,j+1)とD(2,j+1)を入れ替えたものである。ここでｊはｊ＝２×ｍ＋１、ｍはｍ≧０の任意の整数である。

【0119】

この場合、個々の分割データのみでは、それを構成する分割部分データ間で演算を行っても乱数成分が失われない。これは、図６より

D(1,j)*D(1,j+1)=(S(j)*R(j)*R(j+1))*(S(j+1)*R(j+1))

=S(j)*S(j+1)*R(j)*((R(j+1)*R(j+1))

=S(j)*S(j+1)*R(j)*0

=S(j)*S(j+1)*R(j)

D(2,j)*D(2,j+1)=(S(j)*R(j))*(S(j+1)*R(j)*R(j+1))

=S(j)*S(j+1)*(R(j)*R(j))*R(j+1))

=S(j)*S(j+1)*0*R(j+1)

=S(j)*S(j+1)*R(j+1)

D(3,j)*D(3,j+1)=R(j)*R(j+1)

となるからである。

【0120】

また、この場合、３つの分割データのうち２つから、元データを復元することができるという特性は失われていない。これは、D(1)、D(2)を取得してＳを復元する場合には、図６におけるD(1)、D(2)は、図４におけるD(1)、D(2)を構成する分割部分データを入れ替えたものにすぎないので、明らかにこれらから元データを復元することができ、また、D(1)とD(3)またはD(2)とD(3)を取得してＳを復元する場合には、D(3)は乱数のみからなる分割データであるので、D(1)またはD(2)の分割部分データ毎に必要な個数の乱数との排他的論理和演算を行うことにより、乱数部分を消去して元データを復元することができるからで

ある。

【0121】

次に、一旦分割された分割データにさらに乱数を与えて新たな分割データ（再分割データ）を生成する再分割処理について説明する。これは、ユーザが機密情報Ｓを使って所定のサービスを受ける場合の機密情報管理システム１の再分割データ生成部１４、及び端末２の再分割データ生成部２３の機能を説明するものであるが、これに関しても、分割数が３の場合を例に説明する。尚、本実施の形態における再分割処理は、２つの方法があるので、以下、それぞれについて説明する。

【0122】

（乱数追加注入方式）

図７は、乱数追加注入方式におけるデータ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データD(1),D(2),D(3)を取得し（ステップＳ５０１）、次に、再分割の際に用いる乱数R'を発生させる（ステップＳ５０３）。尚、乱数R'に関しては、後述する機密情報管理システム１の動作において、詳しく説明する。

【0123】

次に、分割データD(1),D(2),D(3)それぞれに乱数R'を所定のルールで注入する（ステップＳ５０５）。これは、後述するようなルールにより分割データD(1),D(2),D(3)の分割部分データと乱数R'の乱数部分データの排他的論理和をとり、新たな分割データD'(1),D'(2),D'(3)を生成するものである（ステップＳ５０７）。

【0124】

図８は、元データSを、元データの半分の長さの処理単位ビット長bに基づいて分割数n=3で３分割する場合の分割部分データの定義式、乱数の再注入後の分割部分データの定義式、および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0125】

ここで、分割部分データD(i,j)の定義式について説明する。

【0126】

まず、第１の分割データD(1)に対しては、図６に示すように、第１の分割部分データD(1,1)は、定義式S(1)*R(1)*R(2)で定義され、第２の分割部分データD(1,2)は定義式S(2)*R(2)で定義される。なお、この定義式の一般形は、D(1,j)に対してはS(j)*R(j)*R(j+1)であり、D(1,j+1)に対してS(j+1)*R(j+1)である（jは奇数とする）。

【0127】

また、第２の分割データD(2)に対しては、図６に示すように、D(2,1)はS(1)*R(1)で定義され、D(2,2)はS(2)*R(1)*R(2)で定義される。この定義式の一般形は、D(2,j)に対してはS(j)*R(j)であり、D(2,j+1)に対してはS(j+1)*R(j)*R(j+1)である（jは奇数とする）。

【0128】

更に第３の分割データD(3)に対しては、図６に示すように、D(3,1)はR(1)で定義され、D(3,2)はR(2)で定義される。この定義式の一般形は、D(3,j)に対してはR(j)であり、D(3,j+1)に対してはR(j+1)である（jは奇数とする）。

【0129】

次に、新たな乱数R'注入後の分割部分データD'(i,j)の定義式について説明する。

【0130】

まず、第１の分割データD'(1)に対しては、図８に示すように、第１の分割部分データD'(1,1)は、定義式D(1,1)* R'(1)*R'(2)、即ち、S(1)*R(1)*R(2)*R'(1)*R'(2)で定義され、第２の分割部分データD'(1,2)は、定義式D(1,2)*R'(2)、即ち、S(2)*R(2)* R'(2)で定義される。なお、この定義式の一般形は、D'(1,j)に対してはD(1,j)*R'(j)*R'(j+1)であり、D'(1,j+1)に対してD(1,j+1)*R'(j+1)である（jは奇数とする）。

【0131】

また、第２の分割データD'(2)に対しては、図８に示すように、D'(2,1)はD(2,1)* R'(1)、即ち、S(1)*R(1)* R'(1)で定義され、D'(2,2)はD(2,2)*R'(1)*R'(2)、即ち、S(2)*R(1)* R(2)*R'(1)*R'(2)で定義される。この定義式の一般形は、D'(2,j)に対

してはD(2,j)* R'(j)であり、D'(2,j+1)に対してはD(2,j+1)* R'(j)*R'(j+1)である（jは奇数とする）。

【0132】

また、第３の分割データD'(3)に対しては、図８に示すように、D'(3,1)はD(3,1)* R'(1)、即ち、R(1)* R'(1)で定義され、D'(3,2)はD(3,2)*R'(2)、即ち、R(2)* R'(2)で定義される。この定義式の一般形は、D'(3,j)に対してはD(3,j)* R'(j)*であり、D'(3,j+1)に対してはD(3,j+1)* R'(j+1)である（jは奇数とする）。

【0133】

このように、再分割部分データD'(i,j)はそれぞれ、分割部分データD(i,j)に、分割部分データD(i,j)の定義式で注入されていた乱数部分データR(j)に対応する乱数部分データR'(j)を注入して排他的論理和を計算して求めるものである。

【0134】

次に、図８の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、機密情報管理システム１の元データ復元部１６の機能を説明するものである。

【0135】

まず、分割部分データD'(2,1),D'(3,1)から第１の元部分データS(1)を次のように生成することができる。

【0136】

D'(2,1)*D'(3,1)=(S(1)*R(1)*R'(1))*(R(1)*R'(1))
=S(1)*(R(1)*R(1))*(R'(1)* R'(1))
=S(1)*0*0
=S(1)

また、別の分割部分データから次のように第２の元部分データS(2)を生成することができる。

【0137】

D'(2,2)*D'(3,1)*D'(3,2)=(S(2)*R(1)*R(2)*R'(1)*R'(2))*
(R(1)* R'(1))*(R(2)* R'(2))
=S(2)*(R(1)*R(1))*(R(2)*R(2))*
(R'(1)* R'(1))*(R'(2)* R'(2))
=S(2)*0*0*0*0
=S(2)

一般に、jを奇数として、

D'(2,j)*D'(3,j)=(S(j)*R(j)*R'(j))*(R(j)* R'(j))
=S(j)*(R(j)*R(j))*(R'(j)*R'(j))
=S(j)*0*0
=S(j)

であるから、D'(2,j)*D'(3,j)を計算すれば、S(j)が求まる。

【0138】

また、一般に、jを奇数として、

D'(2,j+1)* D'(3,j)*D'(3,j+1)=(S(j+1)*R(j)*R(j+1)*R'(j)*R'(j+1))*
(R(j)* R'(j))*(R(j+1)* R'(j+1))
=S(j+1)*((R(j)*R(j))*(R(j+1)*R(j+1))*
*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))
=S(j+1)*0*0*0*0
=S(j+1)

であるから、D'(2,j+1)* D'(3,j)*D'(3,j+1)を計算すれば、S(j+1)が求まる。

【0139】

次に、D'(1),D'(3)を取得してSを復元する場合には、次のようになる。

【0140】

$$D'(1,1)*D'(3,1)*D'(3,2)=(S(1)*R(1)*R(2)*R'(1)*R'(2))*(R(1)*R'(1))*(R(2)*R'(2))$$
$$=S(1)*(R(1)*R(1))*(R(2)*R(2))*(R'(1)*R'(1))*(R'(2)*R'(2))$$
$$=S(1)*0*0*0*0$$
$$=S(1)$$

であるから、D'(1,1)*D'(3,1)*D'(3,2)を計算すれば、S(1)が求まる。

【0141】

また同様に、

$$D'(1,2)*D'(3,2)=(S(2)*R(2)*R'(2))*(R(2)*R'(2))$$
$$=S(2)*(R(2)*R(2))*(R'(2)*R'(2))$$
$$=S(2)*0*0$$
$$=S(2)$$

であるから、D'(1,2)*D'(3,2)を計算すれば、S(2)が求まる。

【0142】

一般に、jを奇数として、

$$D'(1,j)*D'(3,j)*D'(3,j+1)=(S(j)*R(j)*R(j+1)*R'(j)*R'(j+1))*(R(j)*R'(j))*(R(j+1)*R'(j+1))$$
$$=S(j)*(R(j)*R(j))*(R(j+1)*R(j+1))*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))$$
$$=S(j)*0*0*0*0$$
$$=S(j)$$

であるから、D'(1,j)*D'(3,j)*D'(3,j+1)を計算すれば、S(j)が求まる。

【0143】

また、一般に、jを奇数として、

$$D'(1,j+1)*D'(3,j+1)=(S(j+1)*R(j+1)*R'(j+1))*(R(j+1)*R'(j+1))$$
$$=S(j+1)*(R(j+1)*R(j+1))*(R'(j+1)*R'(j+1))$$
$$=S(j+1)*0*0$$
$$=S(j+1)$$

であるから、D'(1,j+1)*D'(3,j+1)を計算すれば、S(j+1)が求まる。

【0144】

次に、D'(1),D'(2)を取得してSを復元する場合には、次のようになる。

【0145】

$$D'(1,1)*D'(2,1)=(S(1)*R(1)*R(2)*R'(1)*R'(2))*(S(1)*R(1)*R'(1))$$
$$=(S(1)*S(1))*(R(1)*R(1))*(R'(1)*R'(1))*R(2)*R'(2)$$
$$=0*0*0*R(2)*R'(2)$$
$$=R(2)*R'(2)$$

であるから、D'(1,1)*D'(2,1)を計算すれば、R(2)*R'(2)が求まる。

【0146】

また同様に、

$$D'(1,2)*D'(2,2)=(S(2)*R(2)*R'(2))*(S(2)*R(1)*R(2)*R'(1)*R'(2))$$
$$=(S(2)*S(2))*R(1)*R'(1)*(R(2)*R(2))*(R'(2)*R'(2))$$
$$=0*R(1)*R'(1)*0*0$$
$$=R(1)*R'(1)$$

であるから、D'(1,2)*D'(2,2)を計算すれば、R(1)*R'(1)が求まる。

【0147】

このR(1)*R'(1), R(2)*R'(2)を使用してS(1),S(2)を求める。

【0148】

$$D'(2,1)*R(1)*R'(1)=(S(1)*R(1)*R'(1))*R(1)*R'(1)$$
$$=S(1)*(R(1)*R(1))*(R'(1)*R'(1))$$

=S(1)*0*0
=S(1)

であるから、D'(2,1)*R(1)*R'(1)を計算すれば、S(1)が求まる。

【0149】

また同様に、

D'(1,2)*R(2)*R'(2)=(S(2)*R(2)*R'(2))* R(2)*R'(2)
=S(2)*(R(2)*R(2))* (R'(2)*R'(2))
=S(2)*0*0
=S(2)

であるからD'(2,2)*R(2)*R'(2)を計算すればS(2)が求まる。

【0150】

一般に、jを奇数として、

D'(1,j)*D'(2,j)=(S(j)*R(j)*R(j+1)*R'(j)*R'(j+1))*(S(j)*R(j)*R'(j))
=(S(j)*S(j))*(R(j)*R(j))*(R'(j)*R'(j))*R(j+1) *R'(j+1)
=0*0*0*R(j+1)*R'(j+1)
= R(j+1)*R'(j+1)

であるからD'(1,j)*D'(2,j)を計算すればR(j+1)*R'(j+1)が求まる。

【0151】

また同様に、

D'(1,j+1)*D'(2,j+1)=(S(j+1)* R(j+1)*R'(j+1))*
(S(j+1)*R(j)*R(j+1)* R'(j)*R'(j+1))
=(S(j+1)*S(j+1))*R(j)* R'(j)*
(R(j+1)*R(j+1))*(R'(j+1)* R'(j+1))
=0* R(j)* R'(j)*0*0
= R(j)* R'(j)

であるからD'(1,j+1)*D'(2,j+1)を計算すればR(j)* R'(j)が求まる。

【0152】

このR(j)* R'(j), R(j+1)*R'(j+1)を使用してS(j),S(j+1)を求める。

【0153】

D'(2,j)*R(j)* R'(j)=(S(j)*R(j)*R'(j))*R(j)*R'(j)
=S(j)*(R(j)*R(j))*(R'(j)*R'(j))
=S(j)*0*0
=S(j)

であるからD'(2,j)*R(j)* R'(j)を計算すればS(j)が求まる。

【0154】

また同様に、

D'(1,j+1)*R(j+1)* R'(j+1)=(S(j+1)*R(j+1)*R'(j+1))*R(j+1)* R'(j+1)
=S(j+1)*(R(j+1)*R(j+1))* (R'(j+1)*R'(j+1))
=S(j+1)*0*0
=S(j+1)

であるからD'(1,j+1)*R(j+1)* R'(j+1)を計算すればS(j+1)が求まる。

【0155】

以上、乱数追加注入方式により再分割データを生成した場合には、３つの再分割データD'(1),D'(2),D'(3)のすべてを用いなくても、３つの再分割データのうち、２つの再分割データを用いて上述したように元データを復元することができる。

【0156】

また、乱数追加注入方式においては、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。

【0157】

（乱数書き換え方式）

図９は、乱数書き換え方式におけるデータ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データD(1),D(2),D(3)を取得し（ステップＳ６０１）、次に、再分割の際に用いる乱数R’を発生させる（ステップＳ６０３）。

【0158】

次に、分割データD(1),D(2),D(3)それぞれに乱数R’を上述した乱数追加注入方式により注入する（ステップＳ６０５）。次に、乱数R’を注入された分割データから旧乱数であるRを消去して、新たな再分割データD’(1),D’(2),D’(3)を生成する（ステップＳ６０７，Ｓ６０９）。

【0159】

図１０は、元データSを、元データの半分の長さの処理単位ビット長bに基づいて分割数n=3で３分割する場合の分割部分データの定義式、乱数R’の再注入後の分割部分データの定義式、さらに乱数Rを消去後の分割部分データの定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0160】

本方式においては、ステップＳ６０５までは、上述した乱数追加注入方式と同様であるため、説明は省略し、古い乱数Ｒを消去した分割部分データの定義式について説明する。

【0161】

まず、第１の分割データD’(1)に対しては、図１０に示すように、第１の分割部分データD’(1,1)は、定義式(S(1)*R(1)*R(2)*R’(1)*R’(2))*(R(1)*R(2))、即ち、S(1)* R’(1)*R’(2)で定義され、第２の分割部分データD’(1,2)は、定義式(S(2)*R(2)* R’(2))*R(2)、即ち、S(2)*R’(2)で定義される。なお、この定義式の一般形は、D’(1,j)に対してはS(j) *R’(j)*R’(j+1)であり、D’(1,j+1)に対してS(j+1)*R’(j+1)である（jは奇数とする）。

【0162】

また、第２の分割データD’(2)に対しては、図１０に示すように、D’(2,1)は(S(1)*R(1)* R’(1))* R(1)、即ち、S(1)* R’(1)で定義され、D’(2,2)は(S(2)*R(1)* R(2)*R’(1)*R’(2))*R(1)*R(2)、即ち、S(2)*R’(1)*R’(2)で定義される。この定義式の一般形は、D’(2,j)に対してはS(j)* R’(j)*であり、D(2,j+1)に対してはS(j+1)* R’(j)*R’(j+1)である（jは奇数とする）。

【0163】

また、第３の分割データD’(3)に対しては、図１０に示すように、D’(3,1)は(R(1)* R’(1))*R(1)、即ち、R’(1)で定義され、D’(3,2)は(R(2)* R’(2))* R(2)、即ち、R’(2)で定義される。この定義式の一般形は、D’(3,j)に対してはR’(j)*であり、D(3,j+1)に対してはR’(j+1)である（jは奇数とする）。

【0164】

このように、再分割部分データD’(i,j)はそれぞれ、分割部分データD(i,j)に、分割部分データD(i,j)の定義式で注入されていた乱数部分データR(j)に対応する乱数部分データR’(j)を注入した後、さらに乱数部分データR(j)を消去するように乱数部分データR(j)を注入して排他的論理和を計算し、求めるものである。

【0165】

その結果、もとの分割部分データD(i,j)の定義式において、乱数部分データR(j)を乱数部分データR’(j)に置換したものが、再分割部分データD’(i,j)の定義式となる。

【0166】

次に、図１０の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、機密情報管理システム１の元データ復元部１６の機能を説明するものである。

【0167】

まず、分割部分データD’(2,1),D’(3,1)から第１の元部分データS(1)を次のように生成することができる。

【0168】

D'(2,1)*D'(3,1)=(S(1)*R'(1))*R'(1)
=S(1)*(R'(1)*R'(1))
=S(1)*0
=S(1)

また、別の分割部分データから次のように第２の元部分データS(2)を生成することができる。

【0169】

D'(2,2)*D'(3,1)*D'(3,2)=(S(2)*R'(1)*R'(2))*R'(1)* R'(2)
=S(2)* (R'(1)*R'(1))*(R'(2)* R'(2))
=S(2)*0*0
=S(2)

一般に、jを奇数として、

D'(2,j)*D'(3,j)=(S(j)*R'(j))* R'(j)
=S(j)*(R'(j)*R'(j))
=S(j)*0
=S(j)

であるから、D'(2,j)*D'(3,j)を計算すれば、S(j)が求まる。

【0170】

また、一般に、jを奇数として、

D'(2,j+1)* D'(3,j)*D'(3,j+1)=(S(j+1)*R'(j)*R'(j+1))* R'(j)* R'(j+1)
=S(j+1)*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))
=S(j+1)*0*0
=S(j+1)

であるから、D'(2,j+1)* D'(3,j)*D'(3,j+1)を計算すれば、S(j+1)が求まる。

【0171】

次に、D'(1),D'(3)を取得してSを復元する場合には、次のようになる。

【0172】

D'(1,1)*D'(3,1)*D'(3,2)=(S(1)*R'(1)*R'(2))* R'(1)*R'(2)
= S(1)*(R'(1)* R'(1))* (R'(2)* R'(2))
=S(1)*0*0
=S(1)

であるから、D'(1,1)*D'(3,1)*D'(3,2)を計算すれば、S(1)が求まる。

【0173】

また同様に、

D'(1,2)* D'(3,2)=(S(2)*R'(2))*R'(2)
=S(2)*(R'(2)*R'(2))
=S(2)*0
=S(2)

であるから、D'(1,2)* D'(3,2)を計算すれば、S(2)が求まる。

【0174】

一般に、jを奇数として、

D'(1,j)*D'(3,j)*D'(3,j+1)=(S(j)*R'(j)*R'(j+1))* R'(j)*R'(j+1)
=S(j)*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))
=S(j)*0*0
=S(j)

であるから、D'(1,j)*D'(3,j)*D'(3,j+1)を計算すれば、S(j)が求まる。

【0175】

また、一般に、jを奇数として、

D'(1,j+1)* D'(3,j+1)=(S(j+1)*R'(j+1)) *R'(j+1)

=S(j+1)*(R'(j+1)*R'(j+1))
=S(j+1)*0
=S(j+1)

であるから、D'(1,j+1)* D'(3,j+1)を計算すれば、S(j+1)が求まる。

【0176】

次に、D'(1),D'(2)を取得してSを復元する場合には、次のようになる。

【0177】

D'(1,1)*D'(2,1)=(S(1)* R'(1)*R'(2))*(S(1)*R'(1))
=(S(1)*S(1))*(R'(1)*R'(1))*R'(2)
=0*0* R'(2)
= R'(2)

であるから、D'(1,1)*D'(2,1)を計算すれば、R'(2)が求まる。

【0178】

また同様に、

D'(1,2)*D'(2,2)=(S(2)*R'(2))*(S(2)*R'(1)*R'(2))
=(S(2)*S(2))*(R'(2)*R'(2))*R'(1)
=0*0*R'(1)
= R'(1)

であるから、D'(1,2)*D'(2,2)を計算すれば、R'(1)が求まる。

【0179】

このR'(1)， R'(2)を使用してS(1),S(2)を求める。

【0180】

D'(2,1)* R'(1)=(S(1)*R'(1))* R'(1)
=S(1)*(R'(1)*R'(1))
=S(1)*0
=S(1)

であるから、D'(2,1)* R'(1)を計算すれば、S(1)が求まる。

【0181】

また同様に、

D'(1,2)*R'(2)=(S(2)*R'(2))* R'(2)
=S(2)* (R'(2)*R'(2))
=S(2)*0
=S(2)

であるからD'(1,2)* R'(2)を計算すればS(2)が求まる。

【0182】

一般に、jを奇数として、

D'(1,j)*D'(2,j)=(S(j)*R'(j)*R'(j+1))*(S(j)* R'(j))
=(S(j)*S(j))*(R'(j)*R'(j)) *R'(j+1)
=0*0*R'(j+1)
= R'(j+1)

であるからD'(1,j)*D'(2,j)を計算すればR'(j+1)が求まる。

【0183】

また同様に、

D'(1,j+1)*D'(2,j+1)=(S(j+1)* R'(j+1))* (S(j+1)*R'(j)*R'(j+1))
=(S(j+1)*S(j+1))*(R'(j+1)* R'(j+1))*R'(j)
=0*0*R'(j)
=R'(j)

であるからD'(1,j+1)*D'(2,j+1)を計算すればR'(j)が求まる。

【0184】

このR'(j)， R'(j+1)を使用してS(j),S(j+1)を求める。

【0185】
D'(2,j)*R'(j)=(S(j)* R'(j))* R'(j)
=S(j)*(R'(j)*R'(j))
=S(j)*0
=S(j)
であるからD'(2,j)*R'(j)を計算すればS(j)が求まる。
【0186】
また同様に、
D'(1,j+1)* R'(j+1)=(S(j+1)* R'(j+1))*R'(j+1)
=S(j+1)* (R'(j+1)*R'(j+1))
=S(j+1)*0
=S(j+1)
であるからD'(1,j+1)* R'(j+1)を計算すればS(j+1)が求まる。
【0187】
以上、乱数書き換え方式により再分割データを生成した場合には、３つの再分割データD'(1),D'(2),D'(3)のすべてを用いなくても、３つの再分割データのうち、２つの再分割データを用いて上述したように元データを復元することができる。
【0188】
また、乱数書き換え方式においても、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。
【0189】
＜動作＞
次に、本実施の形態に係る機密情報管理システム１が適用されるコンピュータシステム１０全体の動作について説明する。ここで、図１１は、ユーザが機密情報Ｓを機密情報管理システム１に登録する動作を説明するシーケンス図であり、図１２は、ユーザがサービスを利用する時の機密情報管理システム１及び端末２の動作を説明するシーケンス図である。
【0190】
（１）　機密情報登録処理
まず、ユーザが端末２から機密情報管理システム１に機密情報Ｓを送信（又は送付）する（ステップＳ１０）。機密情報システム１は、機密情報Ｓと同じ長さの真性乱数Ｒを生成し、該真性乱数Ｒ及び機密情報Ｓから、上述した秘密分散法Ａを用いて３つのデータ（分割データ）D(1),D(2),D(3)を生成する（ステップＳ２０，Ｓ３０）。例えば、具体的には、
D(1)＝（S(1)*R(1)* R(2)）‖（S(2)*R(2)）
D(2)＝（S(1)*R(1)）‖（S(2)*R(1)*R(2)）
D(3)＝R(1)‖R(2)
が生成される。ただし、‖は、ビット列とビット列との結合を意味する。
【0191】
次に、機密情報管理システム１は、r_0＝ｈ（D(3)）を初期情報（乱数種初期値）として生成する（ステップＳ４０）。尚、ｈはハッシュ関数を表し、具体的には、ＳＨＡ－１、ＳＨＡ－２５６、ＳＨＡ－５１２などであり、任意の長さのデータから、それぞれ128ビット、256ビット、及び512ビットのハッシュ値を生成するようになっている。また、本実施の形態におけるハッシュ値ｈ（D(3)）のデータの長さは、後述する疑似乱数アルゴリズムＧのシードの長さ以上であればよい。
【0192】
次に、機密情報管理システム１は、このようにして生成された分割データD(1)及びD(2)をそれぞれ保管サーバ３ａ及び３ｂに送信し、分割データD(3)及び初期情報r_0を端末２に送信（又は送付）する（ステップＳ５０）。

【0193】
これにより、端末２は、送信されてきた分割データD(3)及び初期情報r_0をハードディスク等の記憶装置に記憶するとともに（ステップＳ６０）、保管サーバ３ａ及び３ｂは、それぞれ送信されてきた分割データD(1),D(2)をハードディスク等の記憶装置に記憶する（ステップＳ７０）。また、機密情報管理システム１は、初期情報r_0をハードディスク等の記憶装置に記憶する（ステップＳ８０）。
【0194】
最後に、機密情報管理システム１は、真性乱数Ｒを消去し、カウンタ値ｎを十分に大きい値、例えば、ｎ＝１００と設定して、記憶装置に記憶する（ステップＳ１００，Ｓ１１０）。
【0195】
（２）サービス利用処理
ユーザがサービス提供システム５を利用する場合には、まず、ユーザは機密情報Ｓの使用を機密情報管理システム１に対して要求する（ステップＳ２１０）。これは、端末２から機密情報Ｓの使用を要求する旨をオープンな通信ネットワーク４ｂを介して機密情報管理システム１に送信するものである。
【0196】
機密情報管理システム１は、端末２から機密情報Ｓの使用要求を受け取ると、カウンタ値ｎを記憶装置から取得して、端末２に送信する（ステップＳ２２０）。これにより、機密情報管理システム１及び端末２においては、上述した秘密分散法Ｓを用いて同期がとられた再分割データを生成する。
【0197】
機密情報管理システム１においては、カウンタ値ｎ及び乱数種初期値r_0を用いて乱数種情報$r_n=h^n(r_0)$を生成する（ステップＳ２３０）。尚、$r_n=h(r_{n-1})$であり、例えば、$r_1=h(r_0)$、$r_2=h(h(r_0))$、$r_3=h(h(h(r_0)))$…であり、ｎ＝１００のときには、r_0に対してハッシュ値を１００回求めることになる。
【0198】
次に、所定の疑似乱数生成アルゴリズムＧを用いて、乱数種情報r_nから、機密情報Ｓと同じ長さの疑似乱数Ｒ’（＝Ｇ（r_n））を生成する（ステップＳ２４０）。尚、乱数種情報r_nのデータの長さが、疑似乱数アルゴリズムＧの乱数生成に用いられるシードの長さより長い場合には、例えば、ハッシュ値の先頭からシードの長さ分だけ取り出すなど、データ長の調節を行う。
【0199】
次に、保管サーバ３ａ及び３ｂから取得した分割データD(1)及びD(2)、並びに疑似乱数Ｒ’から上述した秘密分散法Ａを用いて再分割データD’(1)及びD’(2)を生成する（ステップＳ２５０，Ｓ２６０）。尚、データ再分割の方法は、乱数追加注入方式及び乱数書き換え方式のいずれでもよいが、乱数追加注入方式の場合には、例えば、具体的には、
D’(1)＝(D(1,1)*R’(1)* R’(2)) ‖ (D(1,2)*R’(2))
D’(2)＝(D(2,1)*R’(1)) ‖ (D(2,2)*R’(1)*R’(2))
が生成される。
【0200】
次に、機密情報管理システム１は、分割データD(1)及びD(2)に代えて、保管サーバ３ａ及び３ｂに再分割データD’(1)及びD’(2)をそれぞれ記憶させる（ステップＳ２７０）。
【0201】
一方、端末２においても、機密情報管理システム１から送信されたカウンタ値ｎ及び乱数種初期値r_0を用いて、機密情報管理システム１と同様に、乱数種情報$r_n=h^n(r_0)$を生成する（ステップＳ２８０）。
【0202】
次に、所定の疑似乱数生成アルゴリズムＧを用いて、機密情報管理システム１と同様に

、乱数種情報r_nから、機密情報Ｓと同じ長さの疑似乱数Ｒ’（＝Ｇ（r_n））を生成する（ステップＳ２９０）。尚、乱数種情報r_nのデータの長さが、疑似乱数アルゴリズムＧの乱数生成に用いられるシードの長さより長い場合には、例えば、ハッシュ値の先頭からシードの長さ分だけ取り出すなど、データ長の調節を行う。

【0203】

次に、分割データD(3)及び疑似乱数Ｒ’から上述した秘密分散法Ａを用いて再分割データD’(3)を生成する（ステップＳ３００）。尚、乱数追加注入方式の場合には、例えば、具体的には、

D’(3)＝(D(3,1)*R’(1))‖(D(3,2)*R’(2))

が生成される。

【0204】

次に、端末２は、分割データD(3)に代えて、記憶装置に再分割データD’(3)を記憶させるとともに、再分割データD’(3)を機密情報管理システム１にオープンな通信ネットワーク４ｂを介して送信する（ステップＳ３１０，Ｓ３２０）。

【0205】

これにより、機密情報管理システム１は、同期がとられた再分割データD’(1),D’(2),D’(3)を取得するので、再分割データD’(1)，D’(2),D’(3)のいずれか２つから秘密分散法Ａを用いて機密情報Ｓを復元する（ステップＳ３３０）。そして、復元した機密情報Ｓをセキュアな通信ネットワーク４ａを介してサービス提供システム５に送信する（ステップＳ３４０）。

【0206】

サービス提供システム５は、機密情報管理システム１から機密情報Ｓを受け取ると、該機密情報Ｓの正当性を判断して、端末２に通信ネットワーク４を介してサービス提供を行う（ステップＳ３５０，Ｓ３６０）。これにより、ユーザは所望のサービスの提供を受けることができる。

【0207】

最後に、機密情報管理システム１は、カウンタ値ｎを１減算し（例えば、ｎ＝１００の場合には、ｎ＝９９になる）、更新されたカウンタ値を記憶装置に記憶させる（ステップＳ３７０，Ｓ３８０）。

【0208】

従って、ユーザが次回、機密情報Ｓを使ってサービス提供システム５を利用する場合には、１減算されたカウンタ値をもとに再分割データD’(1)，D’(2),D’(3)が生成されることになる。尚、カウンタ値ｎが０となったときは、再度、機密情報登録処理のステップＳ２０～Ｓ１１０の処理を実行した後、上記サービス利用処理を実行するものである。

【0209】

次に、サービス利用時に端末２から送信される再分割データD’(3)が、仮に第３者に盗聴されたとしても、なりすましが不可能であることを以下に示す。

【0210】

定義より、D’(3)＝(D(3,1)*R’(1))‖(D(3,2)*R’(2))

ここで、D’(3)の前半部と後半部とを別々に排他的論理和（XOR）を計算するのも、前半部と後半部を連接したものに排他的論理和（XOR）を計算するのも結果は同じであるため、

D’(3)＝(D(3,1)‖D(3,2))*(R’(1)‖R’(2))

＝R*R’

＝R*Ｇ（r_n）

＝R*Ｇ（h^n（r_0））

この結果から、第３者がD’(3)を盗聴して、仮にD’(3)からＲ、r_0を算出し、疑似乱数アルゴリズムＧを把握できれば、上述したサービス利用処理のステップＳ２１０～Ｓ３１０を実行することで、送信すべき再分割データD’(3)を求めることはできるが、実際には、Ｒは真性乱数であり数式等に基づく規則性がないため、D’(3)を盗聴しても、Ｇ（

$h^n(r_0)$）を特定することができない。これは、バーナム暗号（データと同じ長さの乱数列を用意し、暗号化に際してはデータのｎビット目と乱数列のｎビット目の排他的論理和（XOR）を計算し、復号化に際しては暗号化されたデータのｎビット目と乱数列のｎビット目の排他的論理和（XOR）を計算する暗号）は、いくら計算リソースがあっても鍵となる乱数列がなければデータを得ることができないことに起因する。また、Ｒが真性乱数でなく（上記実施の形態においては好適な形態として真性乱数を用いたが、疑似乱数を用いた場合）、仮に、$G(h^n(r_0))$が特定でき、さらに疑似乱数アルゴリズムＧのシード$h^n(r_0)$が逆算できたとしても、ハッシュ関数は一方向性関数であるため、r_0を計算することはできず、結局のところ、第３者のなりすましは不可能である。

【0211】

従って、本実施の形態によれば、機密情報を秘密分散法Ａを用いて複数に分割して、そのうちの一部をユーザに保持させるとともに、機密情報を使用するたびに、各分割データを同期をとって更新して再分割データを生成するので、仮にユーザが保持する機密情報の一部が第３者に漏洩したとしても、第３者のなりすましを確実に防止することができ、セキュリティを十分に確保することができる。

【0212】

特に、本発明における秘密分散法Ａは、機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するので、機密情報を復元することなく、機密情報を再分割することができるので、ユーザの機密情報をよりセキュアに管理することができる。所定のサービスを受ける際に必要とされる機密情報Ｓを秘密分散法Ａを用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割データの紛失があったとしても、残りの分割データから機密情報Ｓを復元できるとともに、秘密分散法Ａを用いて新たに再分割データを生成し、該再分割データの一部を新たにユーザに保持させるので、機密情報Ｓの変更は不要である。

【0213】

尚、本実施の形態における秘密分散法Ａは、多項式演算・剰余演算などを含む多倍長整数の演算処理を必要としないので、大容量データを多数処理する場合においても簡単かつ迅速にデータの分割および復元を行うことができるという効果を得ることができる。

【0214】

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、機密情報管理システム１が端末２にカウンタ値ｎを送信することにより、機密情報管理システム１と端末２の同期をとっていたが、本発明において同期をとる方法はこれに限定されず、減少する同期値を用いるのであれば、他の方法であってもよい。例えば、機密情報管理システム１及び端末２それぞれの時計を同じ時刻に合わせるとともに、ｎを所定の時期（例えば、具体的には、２００４年１２月３１日）までの残りの秒数として同期をとるようにしてもよい。

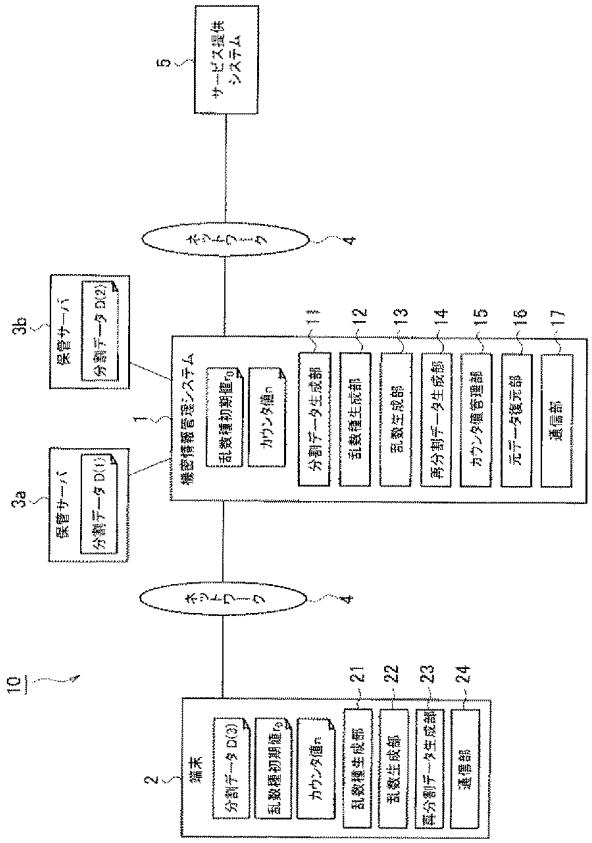
【0215】

また、本実施の形態においては、乱数種初期値r_0を$r_0=h(D(3))$とし、分割データD(3)に依存するように設定したが、乱数種初期値r_0を分割データに依存させず、独立に所定の値を与えてもよいものである。

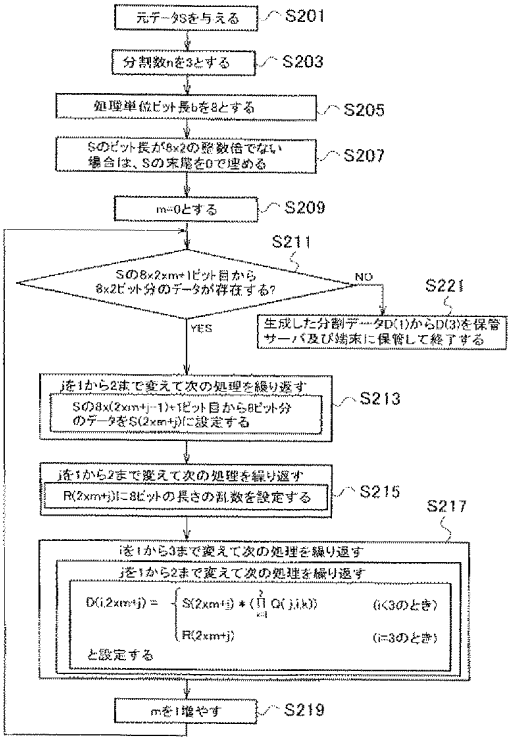
【図面の簡単な説明】

【0216】
【図1】本発明の実施の形態に係る機密情報管理システムが適用されるコンピュータシステム全体の概略構成を示すブロック図である。
【図2】本発明の実施の形態に係る機密情報管理システムの分割数ｎ＝３の場合の分割処理を示すフローチャートである。
【図3】１６ビットの元データSを８ビットの処理単位ビット長に基づいて分割数n=3で３分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。
【図4】分割数n=3の場合の分割データ、分割部分データ、各分割部分データを生成する定義式を示す表である。
【図5】本発明の実施の形態に係る機密情報管理システムの分割数がｎで処理単位ビット長がｂである場合の一般的な分割処理を示すフローチャートである。
【図6】分割数n=3の場合の分割データ、分割部分データ、各分割部分データを生成する定義式の別の例を示す表である。
【図7】本発明の実施の形態に係る機密情報管理システムにおけるデータ再分割処理（乱数追加注入方式）を示すフローチャートである。
【図8】乱数追加注入方式により元データSを元データSの半分の長さの処理単位ビット長に基づいて分割数n=3で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。
【図9】本発明の実施の形態に係る機密情報管理システムにおけるデータ再分割処理（乱数書き換え方式）を示すフローチャートである。
【図10】乱数書き換え方式により元データSを元データSの半分の長さの処理単位ビット長に基づいて分割数n=3で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。
【図11】本発明の実施の形態に係る機密情報管理システムにおいて機密情報を登録する処理を説明するシーケンス図である。
【図12】本発明の実施の形態に係る機密情報管理システムにおいてサービス利用時の処理を説明するシーケンス図である。
【符号の説明】
【0217】
１…機密情報管理システム
２…端末
３ａ，３ｂ…保管サーバ
４…通信ネットワーク
５…サービス提供システム
１０…コンピュータシステム
１１…分割データ生成部
１２…乱数種生成部
１３…乱数生成部
１４…再分割データ生成部
１５…カウンタ値管理部
１６…元データ復元部
１７…通信部
２１…乱数種生成部
２２…乱数生成部
２３…再分割データ生成部
２４…通信部

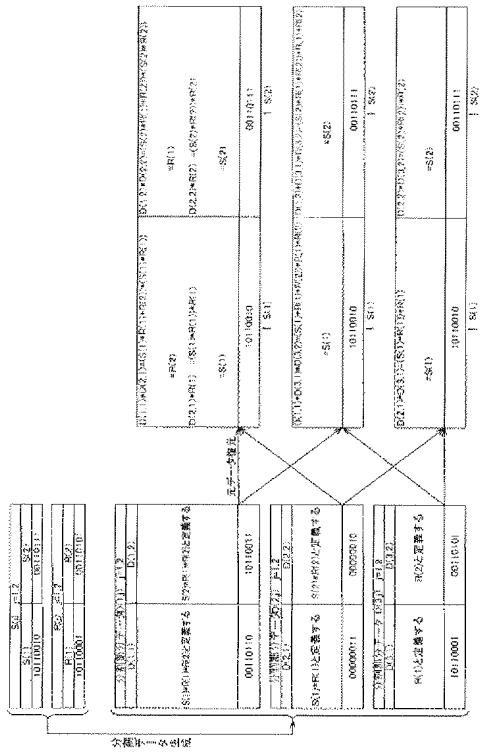
【図1】


5
サービス提供システム
ネットワーク
4
3b
保管サーバ
分割データ D(2)
1
機密情報管理システム
乱数種初期値r0
カウンタ値n
分割データ生成部
乱数種生成部
乱数生成部
再分割データ生成部
カウンタ値管理部
元データ復元部
通信部
11
12
13
14
15
16
17
3a
保管サーバ
分割データ D(1)
ネットワーク
4
10
2
端末
分割データ D(3)
乱数種初期値r0
カウンタ値n
乱数種生成部
乱数生成部
再分割データ生成部
通信部
21
22
23
24

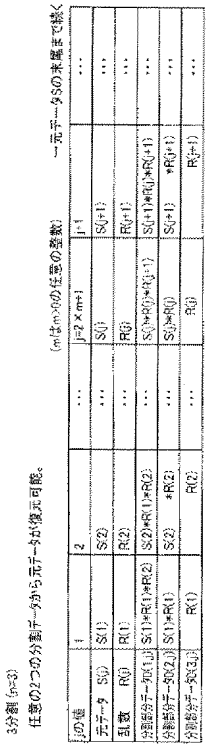
【図2】


元データSを与える
S201
分割数nを3とする
S203
処理単位ビット長bを8とする
S205
Sのビット長が8x2の整数倍でない場合は、Sの末尾を0で埋める
S207
m=0とする
S209
S211
Sの8x2xm+1ビット目から8x2ビット分のデータが存在する?
NO
YES
S221
生成した分割データD(1)からD(3)を保管サーバ及び端末に保管して終了する
jを1から2まで変えて次の処理を繰り返す
S213
Sの8x(2xm+j-1)+1ビット目から8ビット分のデータをS(2xm+j)に設定する
jを1から2まで変えて次の処理を繰り返す
R(2xm+j)に8ビットの長さの乱数を設定する
S215
S217
iを1から3まで変えて次の処理を繰り返す
jを1から2まで変えて次の処理を繰り返す
D(i,2xm+j) =
S(2xm+j) * (∏ Q(j,k))
(i<3のとき)
R(2xm+j)
(i=3のとき)
と設定する
mを1増やす
S219

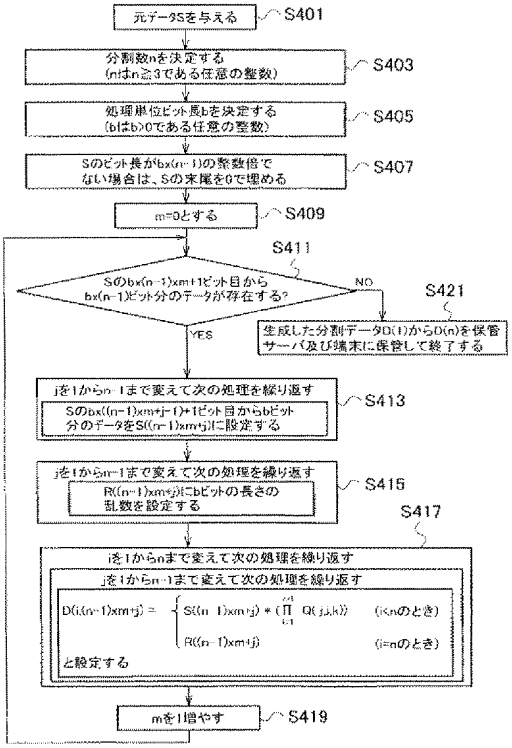
【図3】



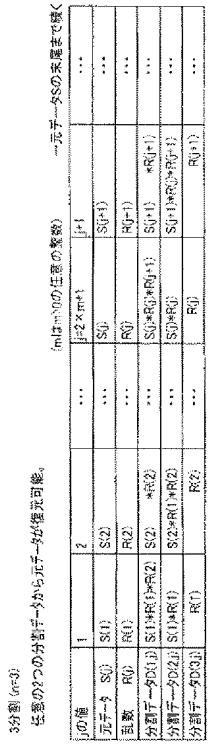
【図4】


～元データSの末尾まで続く
(mは0からの任意の整数)
3分割 (n=3)
任意の2つの分割データから元データSが復元可能。

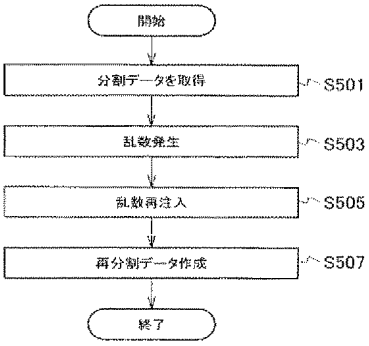
【図5】


元データSを与える
S401
分割数nを決定する
(nはn≧3である任意の整数)
S403
処理単位ビット長bを決定する
(bはb>0である任意の整数)
S405
Sのビット長がbx(n-1)の整数倍で
ない場合は、Sの末尾を0で埋める
S407
m=0とする
S409
S411
Sのbx(n-1)xm+1ビット目から
bx(n-1)ビット分のデータが存在する?
NO
YES
S421
生成した分割データD(1)からD(n)を保管
サーバ及び端末に保管して終了する
jを1からn-1まで変えて次の処理を繰り返す
Sのbx((n-1)xm+j-1)+1ビット目からbビット
分のデータをS((n-1)xm+j)に設定する
S413
jを1からn-1まで変えて次の処理を繰り返す
R((n-1)xm+j)にbビットの長さの
乱数を設定する
S415
S417
iを1からnまで変えて次の処理を繰り返す
jを1からn-1まで変えて次の処理を繰り返す
D(i,(n-1)xm+j) = S((n-1)xm+j) * (∏ Q(j,k)) (i<nのとき)
R((n-1)xm+j) (i=nのとき)
と設定する
mを1増やす
S419

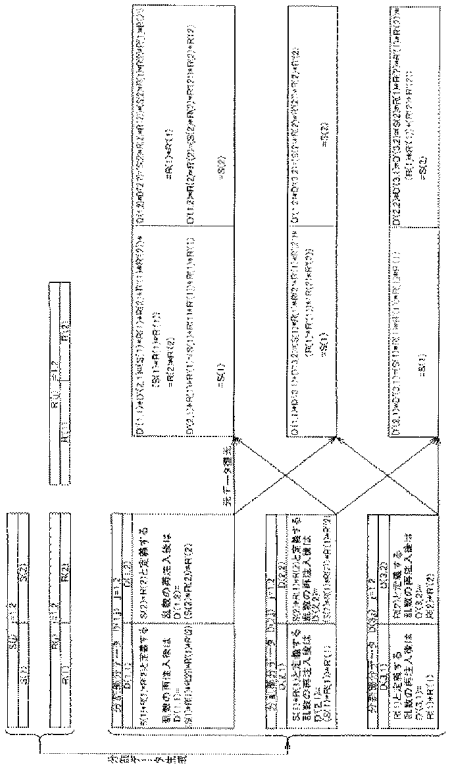
【図6】


3分割 (n=3)
任意の2つの分割データから元データが復元可能。
(mは1つの任意の整数)
元データSの末尾まで繰り返す
jの値
1
2
j
j+1
2×m+1
元データ S(j) S(1) S(2) S(j) S(j+1)
乱数 R(j) R(1) R(2) R(j) R(j+1)
分割データD(1,j) S(1)*R(1)+R(2) S(2) *R(2) S(j)*R(j)+R(j+1) S(j+1) *R(j+1)
分割データD(2,j) S(1)*R(1) S(2)*R(1)+R(2) S(j)*R(j) S(j+1)*R(j)+R(j+1)
分割データD(3,j) R(1) R(2) R(j) R(j+1)

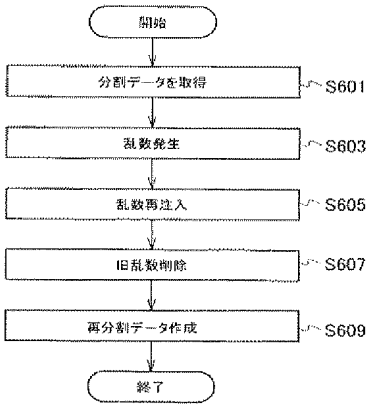
【図7】


開始
分割データを取得
S501
乱数発生
S503
乱数再注入
S505
再分割データ作成
S507
終了

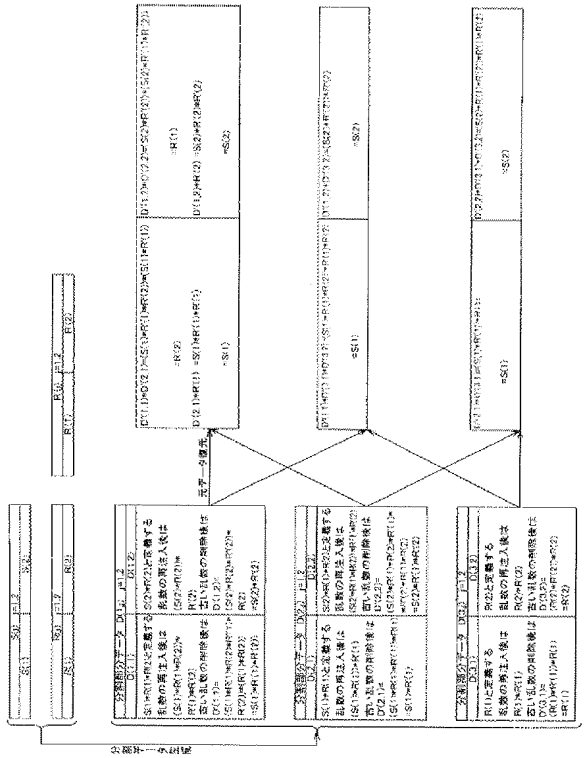
【図8】



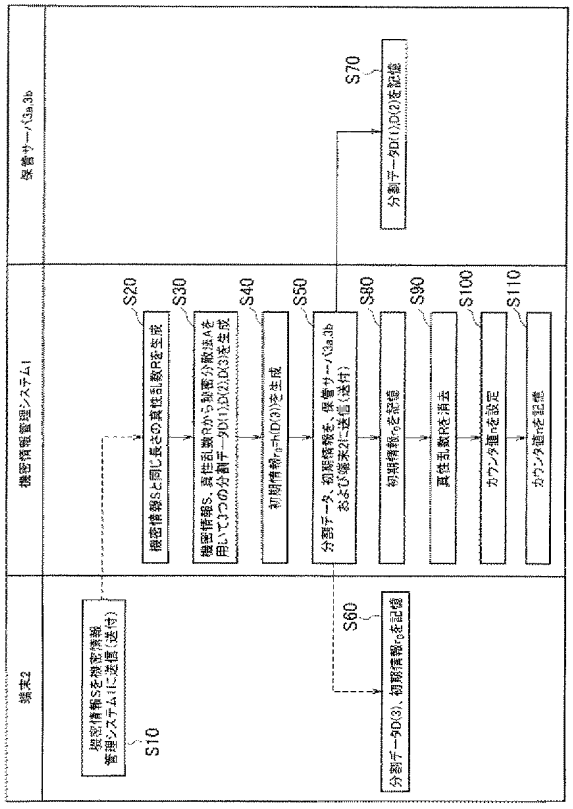
【図9】



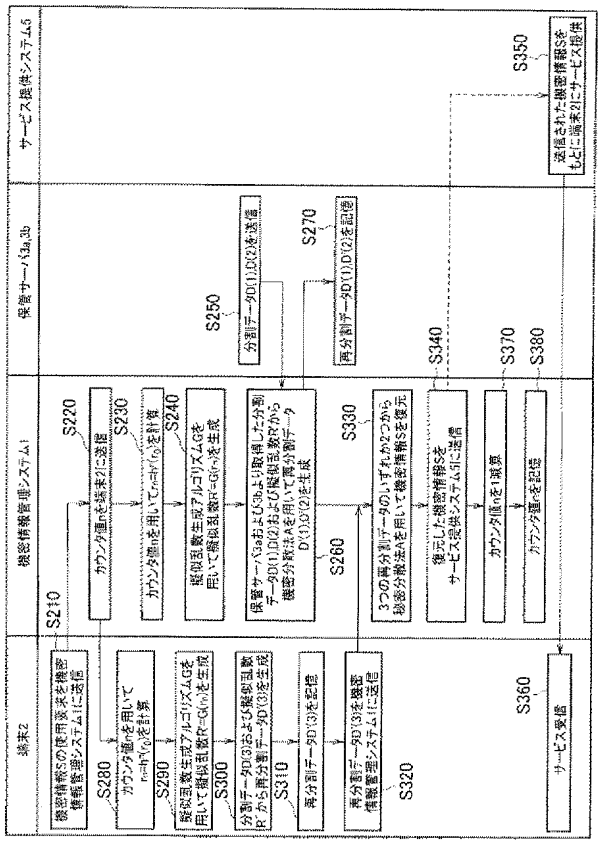
【図10】



【図11】



【図12】



(72)発明者　荻原　利彦
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　加賀谷　誠
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　野村　進
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
Ｆターム(参考)　5B017 BA05　BA10
5J104 AA12　NA12　PA14